The Commonwealth of Massachusetts

AUDITOR OF THE COMMONWEALTH

STATE HOUSE, BOSTON 02133

No. 97-7055-4W

REPORT ON THE PREPAREDNESS OF THE COMMONWEALTH OF MASSACHUSETTS TO ADDRESS THE YEAR 2000 COMPUTER DATE ISSUE

April 17, 1997 to October 21, 1997

A. Joseph DeNucci, Auditor
The Office of the State Auditor
Information Technology Audit Division

The Commonwealth of Massachusetts

AUDITOR OF THE COMMONWEALTH

STATE HOUSE, BOSTON 02133

A. JOSEPH DeNUCCI
AUDITOR

TEL. (617) 727-2075

97-7055-4W

February 3, 1998

Honorable A. Paul Cellucci, Governor
Honorable Thomas F. Birmingham, President of the Senate
Honorable Thomas M. Finneran, Speaker of the House of Representatives
Honorable Stanley C. Rosenberg, Chairman of the Senate Committee on Ways and Means
Honorable Paul R. Haley, Chairman of the House Committee on Ways and Means
Honorable David P. Magnani, Senate Committee on Science and Technology
Honorable Lida E. Harkins, House Committee on Science and Technology
Honorable Members of the General Court

I am presenting this report on how prepared the Commonwealth of Massachusetts is to address the year 2000 computer date issue. Our survey was undertaken to identify the extent to which state agencies and authorities of the Commonwealth have assessed the impact of year 2000 on their automated systems and technology and have taken steps to make essential information systems year 2000 compliant.

Clearly, the upcoming change of century poses a serious risk to virtually all business and operational functions that rely on computer systems and technology. Over the past year or so, the year 2000 issue has received a great deal of attention. As in the private sector, there is much to be done within the Commonwealth to avoid the disruption of essential state-provided services. With that in mind, I would like to share with you the results of my survey and to present recommendations to assist the Commonwealth in addressing this significant issue.

The year 2000 problem stems from the fact that, to conserve electronic data storage space, practically all computer systems have used two digits to represent the year. A problem arises when dates beyond 1999 are used, because the computer system cannot distinguish the century. It cannot tell the difference between 1900 and 2000, because both would be represented by "00." As a result, if not modified, computer systems that use dates or perform date or time-sensitive calculations may generate incorrect results beyond the year 1999. In fact, such problems have already occurred because dates affect calculations that project into the next century.

The dimensions of the year 2000 problem for the Commonwealth are enormous. Practically every single automated system and its related technology, regardless of size, is impacted. Given our heavy reliance on computer systems, their failure to operate properly could mean anything from minor inconveniences to major problems. Virtually all citizens and businesses in the Commonwealth would be affected should state systems supporting our ability to collect revenue, pay bills, provide benefits, and support health, safety, and educational services be adversely impacted by the year 2000 problem.

It is without doubt a major challenge just to identify which systems and technology will be affected and determine the extent of year 2000 impact on them. It is as important, and even more difficult to develop appropriate strategies, to obtain the required resources and expertise, to provide sufficient testing, and to implement corrected code. In this regard, it is of concern that nearly 42% of the entities responding to our survey had not begun efforts to address the year 2000 problem. Agencies that have not yet begun to address the year 2000 problem must begin to do so now, giving special attention to those systems that will require contingency plans. Correcting the year 2000 problem will be labor-intensive and time-consuming and will require additional resources not sufficiently available within state government. Further, resolving the problem must be accomplished without interrupting current state services.

Ironically, the enormous challenge involved in achieving year 2000 compliance is not technical, but managerial. Whether agencies succeed or fail will be largely influenced by the quality of the executive leadership and the use of strong project management techniques. It is imperative that senior management, including the secretariat information officer, the agency head, and the agency's chief information officer, are fully aware of the year 2000 effort and that they communicate its importance to all agency personnel in such a way that everyone understands why the issue is so important. Management must also ensure that this understanding is translated into corrective action.

A state agency's ability to successfully manage its year 2000 program will also depend on the degree to which the agency has institutionalized key systems development and program management techniques and on its experience in managing large-scale software conversion or systems development efforts. The OSA's Information Technology Audit Division has reported on numerous occasions that agencies need to address and improve their management of information technology. Accordingly, to carry out their year 2000 programs, agencies need to assess their information management capabilities, resources, and techniques and, if necessary, upgrade them. In the process, agencies should consider soliciting assistance from organizations experienced in managing major software conversions.

I want to thank the many state officials and employees who responded to the survey, or provided input through interviews, and the Information Technology Division of the Executive Office of Administration and Finance for their assistance.

Should you have any questions or, concerns regarding this report, we would be pleased to provide any additional information required. I look forward to continuing to work with you on this and other important issues affecting the quality of services provided by the Commonwealth.

Sincerely,

A. Joseph DeNucci
Auditor of the Commonwealth

TABLE OF CONTENTS

INTRODUCTION

Background

In the near future, if not already, computer systems originally programmed to process dates using two digits to represent the year will either make gross errors in calculations or will not function when processing dates in the year 2000 and beyond. If these computer systems have not been properly modified to process dates in year 2000 and beyond, the systems will be unable to perform date-related calculations or may crash. In fact, such problems will surface well before January 1, 2000, because calculations required at present project into the next century. Due to the tremendous reliance placed on automated systems to support business functions in government, the failure to process, or to process correctly, could have a devastating impact on those doing business with or depending on the services of the Commonwealth.

Dates are critical to the integrity of computer systems and the information they provide. Not only do computers have internal clocks that are an integral part of their operating systems and certain system software; the vast majority of information processing is date-dependent. Dates are used to identify economic events and records of actions taken and to process calculations of past and future events.

Ironically, to save storage space and data entry costs, programmers in the past used two digits to designate years occurring in the 1900s. Most computer systems represent dates in the format MMDDYY, where 123197 would represent December 31, 1997. Here, the century is not specifically represented in the date format. Rather, it is understood that a date such as 12/31/97 is in the twentieth century. In order for a date to define a year beyond the twentieth century, a four-digit code for the year would be necessary. Over time, application systems projecting dates beyond 1999 confronted the impasse of the two-digit code. In such situations, modifying the application software largely solved the problem. Except for this small number of modified systems, the vast majority of computer programs currently perform arithmetic and logic operations on date fields using only two digits for the year. As long as the dates were in the same century, as they have been, the program would work as intended. However, problems have arisen when application systems have been required to use or to calculate with dates projecting into the next century. For example, a computer subtracting 02/03/98 from 02/03/08 to determine someone's age would not produce the correct answer of 10; it would produce a result of -90. However, because date-related calculations are not signed (+/-), the person would appear to be 90 instead of his or her real age of 10.

The magnitude of the year 2000 (or Y2K) problem for the Commonwealth is enormous. The date problem exists for all processing platforms, including mainframes, minicomputers, microcomputers, local area networks (LANs), and telecommunications systems such as private branch exchanges (PBXs). Essentially, the two-digit year field can be found in computer equipment, firmware, operating systems, software compilers, job control language, queries, screens, procedures, calls to other programs, microcode, databases, application systems, and data. Many of the state's computer systems, originally designed and developed 15 to 20 years ago, may not be adequately documented; may use different programming languages; and may operate on a variety of hardware platforms. There are hundreds of computer programs, each with thousands of lines of code to be examined for date problems. Even if the Commonwealth were to completely solve the year 2000 problem for its own systems, data from outside sources that are not in compliance could contaminate them. Government entities or business partners could supply either incorrect data based on erroneous calculations from their systems that have not attained compliance or could supply data using a different date format.

Bringing technology and systems into year 2000 compliance is no small job. It has been estimated by analysts at the Gartner Group that the worldwide conversion cost to resolve the year 2000 problem will be up to $600 billion, and other analysts have placed estimates for total global costs at over $1 trillion. In addition, costs have been estimated to be between $50 and $75 billion in the United States, $30 billion of which is for the U.S. federal government. With respect to individual enterprises, it has been estimated that the cost for attaining year 2000 compliance for systems in a large enterprise could reach $40 million. Although the exact cost to be incurred by the Commonwealth has not been determined, it has been estimated to be approximately $50 to $70 million.

The process of making an organization's technology and systems year 2000 compliant begins with assessing the entire IT environment to identify which systems are impacted. To assist, there are software tools that can be useful in identifying where date fields exist in program code and elsewhere. Generally, these software products are of two types. The first group includes products that change the system date for a particular program, thus allowing analysts to see how the program will react when it encounters a twenty-first century date. The second category consists of products that help to identify date fields in program code and trace the flow of dates through a system as they are moved from field to field. Because naming standards do not exist for date fields of all systems, date fields within programs can be called anything, thus making the task of locating date variables difficult, if not impossible in some cases, without a complete code examination.

Although automated tools should make the code conversion process quicker and easier, none of these tools completely eliminates the need to manually review program code for date fields and any associated calculations based on them. Worse yet, some agencies and departments may find that source code (e.g., the English version of the program code that is operating within the computer) for certain systems is not in sync with the executable code or no longer exists. In the event that the source code cannot be found, the object code will need to be decompiled, if possible, to examine the source code version, or a replacement system will need to be developed or acquired.

Once the impact has been assessed, organizations need to identify the systems to be modified, develop a strategy for making the necessary changes, obtain the required resources, initiate remedial action, perform testing, and finally implement the changes. Although there are software products that assist project-cost estimating and cost modeling, editing of actual changes required, program change management, and testing to verify and validate the changed system, state entities also need established standards to follow and expertise upon which to rely.

According to the tenets of good internal control, as outlined in Chapter 647 of the Acts of 1989 and other generally-accepted internal control practices, it is a primary fiduciary responsibility of a state entity's management to ensure the continued integrity of its business operations and to ensure that the entity's assets are adequately safeguarded. Failure to sufficiently address the Commonwealth's year 2000 problem in a timely manner for mission-critical systems could result in a loss of important business processing or corrupt the integrity of automated systems. Citizens and other parties who are dependent on state services could be denied such services, from unemployment compensation to state-provided higher education, state police protection, and welfare benefits.

The seriousness of the year 2000 problem should not be underestimated given our heavy reliance on information technology. Clearly, a great deal is at stake. Citizens and parties doing business with the Commonwealth could be adversely affected should systems on which they directly or indirectly depend lose their integrity. Failure to fully correct the year 2000 problem could result in widespread miscalculations, inability to process state business, and public dismay at a perceived ineptitude on the part of public administrators, not to mention adverse public opinion and the potentially catastrophic legal implications of an interruption in the Commonwealth's business operations.

The Office of the State Auditor's Survey

The Office of the State Auditor (OSA) initiated this survey because of the significance of the year 2000 issue and our perception that little substantive action had been taken by the Commonwealth to address the problem. The intent of our survey was to provide an assessment of the level of year 2000 preparedness and to offer recommendations to assist state entities in addressing the issue.

The objective of our survey questionnaire (see Appendix 1, page 36) was to obtain sufficient information to take a "barometric reading" on the level of preparedness and, in this way, help to heighten the awareness of the problem. Our office mailed, or distributed by other means, 638 questionnaires to state agency heads. The questionnaire was also included as part of an April 1997 year 2000 publication issued by the Executive Office for Administration and Finance's Information Technology Division. The recipients were asked to complete the survey questionnaire and forward it to our office.

The year 2000 issue is a serious problem requiring immediate attention and appropriate actions of senior management, chief financial officers, chief information officers, technology managers, business-process owners, and system users. The purpose of this report is to present the results of our survey and to encourage public officials and state administrators to ensure an adequate allocation of required resources and an appropriate level of management direction to achieve an acceptable level of year 2000 compliance.

SURVEY SCOPE, OBJECTIVES, AND METHODOLOGY

Survey Scope

The scope of our survey was to review state entities regarding their awareness of the year 2000 problem and steps planned or taken to address it with regard to their technology and automated systems. Included in the survey were entities from the executive branch, judiciary, legislative branch, constitutional offices, and independent authorities.

Survey Objectives

A survey questionnaire was used to solicit input regarding the degree to which state entities were aware of the year 2000 problem. The survey was designed to garner information regarding the nature and extent of assessment, planning, and remedial action efforts to address the year 2000 problem. Further, the survey was conducted to determine whether the Commonwealth at large was sufficiently aware of the year 2000 issue and whether steps had been taken to ensure that essential information systems and information technology would attain year 2000 compliance. An additional objective of the survey was that it should serve as an instrument to increase the general level of awareness of the year 2000 issue by requiring state administrators to respond to an array of related questions.

Survey Methodology

To determine the extent of awareness and preparedness for four-digit-year processing for computer operations prior to and subsequent to the year 2000, a ten-page survey was mailed to chief executive officers of 607 state departments, agencies, and authorities. Following the initial response deadline, three complete rounds of telephone calls were made to entities that had not yet responded, encouraging them to do so. We conducted on-site interviews with key administrators from a sample of state entities to obtain more in-depth information regarding their efforts to address the year 2000 problem. In addition, we interviewed the management of the Commonwealth's Information Technology Division (ITD) within the Executive Office for Administration and Finance, which had taken a leadership role regarding year 2000 for executive branch agencies.

The responses to our survey were entered into a database and summarized with the assistance of ITD. To encourage entities to respond, we acknowledged in the survey's cover letter that entities may have been in the early stages of their year 2000 efforts and that the survey was not designed to establish blame on a person or department for non-compliance as of the time of the survey. Accordingly, the report is written from the perspective of the Commonwealth as a whole, recognizing that the extent of progress made may vary significantly among all entities.

EXECUTIVE SUMMARY

The Commonwealth of Massachusetts has been late in its efforts to assess the impact of year 2000 on its automated systems and technology and to initiate steps to achieve year 2000 compliance for those systems. Although some state entities have made good efforts to ensure that their systems will operate correctly when using dates on or after January 1, 2000, the Commonwealth, overall, is not adequately positioned to ensure that all mission-critical and important automated systems and supporting technology will be year 2000 compliant in time. Resource limitations, insufficient project plans regarding what systems and technology are impacted and which need to be modified, and absolute time constraints hinder the ability of many state entities to effectively deal with the year 2000 date problem. At the time of our survey, only 111 of 282 respondents, representing 434 entities and the bulk of state's information technology, had completed their assessments of the year 2000 date problem. Furthermore, only 14 of the 282 responding entities had written, approved year 2000 project plans. Except for a small core of agencies that seem to be effectively addressing the issue, substantial efforts are needed for state systems to attain year 2000 compliance in time.

Our survey indicated that only a relatively small number of state entities had a good understanding of the year 2000 problem and had completed their assessments of impact, developed strategies, and initiated efforts to ensure that their business application systems will achieve year 2000 compliance. There were other state entities that had increased their understanding of the problem within the past six months, and had initiated assessment efforts and were developing plans for making required system modifications. However, for a number of entities, there was little evidence to demonstrate that they were adequately prepared to meet year 2000 deadlines for their information systems and supporting technology. Unless the Commonwealth devotes greater efforts and resources to fully assessing the impact, taking corrective action, and developing viable contingency plans; citizens and others who depend on state services will be adversely affected when necessary systems fail to operate as intended.

Although the awareness of the year 2000 issue has improved across the state, it appears that some governmental entities, senior management, and administrators do not fully understand the associated risks and what needs to be done. In addition, many entities may not have the capacity to successfully address the year 2000 problem. We acknowledge that Administration and Finance's Information Technology Division (ITD), the Department of Revenue, the Legislature's Joint Committee on Science and Technology, and the national and local media have made significant efforts to heighten the awareness of "year 2000." However, there appears to be a segment of state government not adequately aware of the scope of the year 2000 problem or how to address it.

Our survey indicated that the process of performing a detailed analysis of the impact of year 2000 on systems and technology was generally incomplete for the Commonwealth overall. Where assessments had been performed, the process had been focused almost entirely on "traditional" business application systems and to a far lesser degree on all other technology. Except for a limited number of entities, there did not seem to be an adequate understanding that the impact of year 2000 must be evaluated for the entire IT environment -- for all automated systems and technology-supported operations. As a result, the lack of sufficient, detailed information regarding what and how technology is impacted inhibits many Commonwealth entities from formulating appropriate corrective action plans and estimating the total cost.

Ideally, by the time of the survey, impact assessments and compliance plans should have been completed. In addition, necessary remedial actions and the development of contingency plans should have been well underway for systems where there was a reasonable risk of not becoming year 2000 compliant. The survey demonstrated that, in many instances, impact assessments and compliance plans had not been completed, and there was no remedial action or indications that contingency plans were being developed. As a result, it is possible that certain mission-critical and important information systems and technology will not be ready or available when needed.

For most agencies and departments, the year 2000 project will be one of the most challenging and important IT projects undertaken, requiring careful planning and strong project management disciplines. At the outset, administrators need to realistically assess the requirements and availability of resources to evaluate year 2000 impact and to develop, test, and implement appropriate corrective strategies. Agency and department management should be aware that the cost of outsourced services for year 2000 assessment and remedial action will probably rise due to increased competition, and that the quality of services from available resources may diminish as time goes by. The inability of the Commonwealth to establish a realistic, complete estimate for year 2000 remedial action and to develop contingency plans adversely impacts planning for funding and impedes progress on associated required funding requests. As a result, there is a risk that the Commonwealth may not be able to garner the needed resources internally or from the marketplace to accomplish year 2000 compliance and develop workable contingency plans.

Certain state entities not possessing adequate knowledge of the year 2000 problem or how to address it may consider it too overwhelming to address and, as a result, corrective action may not be taken. Other entities, confident that they will address the issue in time, may fall prey to delays caused by significant problems detected during testing and thereby fail to meet their targeted deadlines. Each entity's success or failure must be carefully monitored. Given the high level of importance of technology in supporting government services, we recommend that a system of entity reporting to a centralized unit of state government should be established regarding year 2000 project deliverables and compliance status, and that methods of validation of corrective action should be implemented to track the progress of individual entities and the Commonwealth at large.

Management should be mindful that appropriate internal controls must be exercised when implementing remedial actions. Care must be taken to employ strong control practices when addressing the year 2000 problem under the pressure of elapsing time. We are greatly concerned that, as the century deadline approaches, internal control matters, such as program changes, logical access security to systems and data, and business continuity planning may fall victim to crisis-mode operations and thereby be compromised. Program and data integrity, security, and confidentiality must continue to receive adequate attention appropriate to their importance and sensitivity. Business continuity planning takes on added importance with the real possibility that certain systems may fail to meet the deadline.

Year 2000 is a classic example of an issue impacting the vast majority of all technology serving the Commonwealth, not bounded by platform size or organizational structure. It is also a classic example of an issue for which the Commonwealth would have had an advantage in addressing should a comprehensive enterprise-wide, IT-strategic planning process been in place. Sadly, there are some very real risks involved should critical systems not operate as intended. The failure to have fundamental information on all systems and technology and related year 2000 plans readily available underscores the need for the Commonwealth to have an enterprise-wide, information systems/technology strategic planning process in place.

To ensure that mission critical and important automated systems and technology are year 2000 compliant is no trivial matter. We must establish appropriate points of accountability, fully determine across the Commonwealth what systems and technology must be made year 2000 compliant, develop corrective plans, and employ strong project management techniques. Furthermore, we must determine reliable cost estimates so that funds can be made available in a timely manner. Because assessments and plans are not all complete, it is likely that current estimates of the $50 to $70 million required to address year 2000 may be substantially less than needed.

To assist state entities in addressing the year 2000 problem, this report includes recommendations within the text and listed in Appendix 3, and a Year 2000 Project Tracking Form, see Appendix 6.

Given the importance of year 2000, until significant validation testing has been completed on the overall information systems, their supporting technology and networks, and interfaces with other systems, all systems should be considered at risk of non-compliance. Although there may be systems for which the risk of noncompliance is low, or steadily being reduced, there are a number of systems and technologies for which the likelihood of year 2000 failure remains high.

SURVEY RESULTS

Presented in this section of the report are the results of our survey questionnaire and interviews with ITD and other state entities. The subheadings presented in the section follow the same order of those in the survey questionnaire. The section contains some additional subheadings to provide further guidance to the subject matter. A copy of the survey questionnaire, which includes statistics on responses and review comments for some key questions from our office, begin on page 36. In addition, **recommendations are presented in indented, bold text in this section** and as an action list in Appendix 3, beginning on page 64.

Our office received a total of 282 completed surveys, comprised of 251 mailed questionnaires and 31 from ITD's publication entitled, Year 2000 Meeting the Challenge, dated April 1997. Some of the completed surveys were deemed to represent multiple responses, either because they were stated as such or because certain entities had their data processing services provided by a centralized information technology function at another entity. We determined that 152 additional entities were represented in this manner. Therefore, we ascertained that of the total 638 surveys distributed, 434 or 68%, of the total population of entities were represented in the final responses. Although 32% of the entities failed to respond, those responding represented entities having a substantial portion of the state's information technology.

Given the importance of the "year 2000" problem, it is of concern that almost one third of the surveyed entities failed to respond and, of those who eventually did, only 86 responded by the May 16, 1997 due date (see Figure 1). Shortly after the response deadline, our office initiated a series of telephone calls encouraging those entities that had not yet responded to submit their completed surveys. As Figure 1 indicates, our office received a steady but slow rate of responses until our final cutoff date of October 7, 1997. Our results are, therefore, based upon total responses received by the cutoff date and interviews conducted. Our office

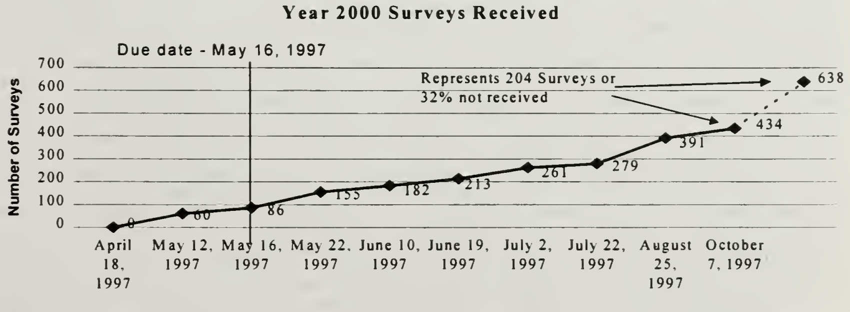


Figure 1

believes that, in part, the slow rate of response, or failure to respond, supports our overall conclusion that the Commonwealth was not sufficiently informed regarding the impact of the year 2000 problem and had not formulated strategic solutions to effectively and efficiently address it.

It is our position that all state administrators should have been aware of the year 2000 issue by early 1997. This was not the case. Our survey indicated that 54, or 19%, of 282 entities responding did not recognize the problem. When added to the 204 of the 638 total entities that did not respond to the survey, we concluded that as many as 40% of all state entities may have been unaware of the year 2000 issue or had not taken sufficient steps to address it. The failure, or slow rate, of returning surveys may also have been the result of a lack of understanding of the problem, or of entities not assigning an employee to address the issue or complete the survey.

Although the survey does raise some serious concerns as to whether all mission-critical and important systems and technology will reach year 2000 compliance in time, there are some positive efforts underway. As indicated by the survey and ITD, certain agencies have already begun to tackle the year 2000 problem. For example, the Office of the State Comptroller has moved forward to ensure that the state's primary accounting information system will be ready in time. The system, known as the Massachusetts Management, Accounting, and Reporting System (MMARS) will be retrofitted for year 2000 compliance at a cost of approximately $2 million. The Office of the State Comptroller had originally intended that, rather than attempting compliance for the Commonwealth's twenty-year old personnel/payroll systems at a cost of $5 million, the Comptroller would replace those systems with new year 2000 compliant hardware and software at a cost approximating $15 million. However, upon becoming aware that new-system conversions could take longer than the time allotted, it was decided that a more prudent approach would be to modify and retrofit the existing systems. In another example, the Department of Revenue has proceeded to attain year 2000 compliance for its systems, and in the process, has led efforts in encouraging year 2000 awareness among other agencies. Although the Division of Employment and Training has a significant effort remaining to complete their year 2000 projects, they have demonstrated a good understanding of the effort required for compliance and have developed an approach for achieving it. Moreover, according to ITD, the Registry of Motor Vehicles, the Department of Correction, and the Office of Child Care Services have achieved compliance on their mission-critical systems, and the Division of Occupational Safety has achieved compliance for its essential systems. At the completion of our survey, ITD stated that, as examples of entities in the process of addressing year 2000, the Operational Services Division (OSD), the Department of Veterans Services, and the Department of Mental Retardation were actively working on their mission-critical systems and had established their target dates for completion as of March 1998.

Certain other agencies and departments for which capital outlay funds for IT have been made available are expected to upgrade or replace their information technology and systems with versions that are year 2000 ready. At the close of our review work, ITD indicated that of 130 agencies they interviewed, 55 stated that they were in compliance or were about to be. Sixty-one of the agencies identified 128 mission-critical systems, 33 of which were in compliance or will be by the first quarter of 1998. Although these statistics may seem encouraging, we remain concerned that large percentage of entities are not yet ready for year 2000 and that ITD's projections have yet to be verified by test results.

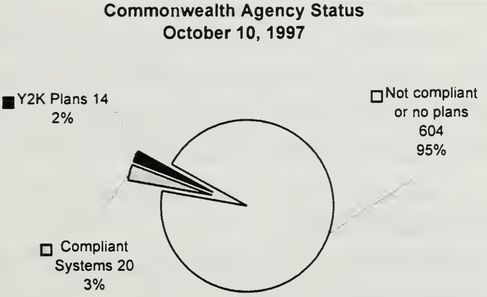


Figure 2

Although progress has also been made by a number of entities since their survey questionnaires were submitted, it appears that only a small core of state entities are likely to successfully address the year 2000 issue in time. The survey results reflect that the vast majority of state entities were just beginning to address the issue. Although other surveys and studies have indicated that the majority of organizations in the public and private sectors have not begun to adequately address year 2000 compliance, little comfort should be taken by this comparison. We urge those who may be waiting for a "silver bullet" not to postpone their efforts.

Since ITD is the primary information systems service provider for the Commonwealth, it has assumed the responsibility of being a centralized clearinghouse for year 2000 issues. Over the past nine months, ITD's Strategic Planning Group (ITD SPG) has established a Year 2000 Program Management Office, formed a state-wide year 2000 users group, hosted awareness programs, established a year 2000 web page, and conducted seminars and workshops to promote best practices for addressing year 2000 compliance. The Year 2000 Program Management Office (Y2K PMO) has coordinated year 2000 activities with our office, the Fiscal Affairs Division (formerly the Budget Bureau), and the Operational Services Division. The Y2K PMO is responsible for coordinating year 2000 activities, promoting awareness, exchanging technical information among the agencies, monitoring statewide efforts on year 2000 progress, and assisting agencies in their year 2000 projects.

> **To coordinate information on the status of year 2000 projects, we recommend that ITD be designated as the central entity to which status reporting from all state agencies and authorities should be submitted. In addition, ITD should establish accreditation methodologies and standards to certify the completion of year 2000 projects.**

Awareness

Although the survey indicated that a relatively high number of entities that responded were aware of the year 2000 problem, given the importance of the issue, the number stating that they were unaware combined with those who left the question blank or failed to respond to the survey was significant at 40%. Although much has been done to improve the level of awareness, remedial action is placed at significant risk for those entities not sufficiently aware of the nature and extent of the problem or how to address it. The survey indicated that state administrators need a more detailed understanding of the year 2000 problem with regard to automated systems and related technology.

It is of concern that for those survey respondents who had indicated a relatively high level of awareness of the year 2000 issue, this awareness had not translated, in most instances, into action plans sufficient to address the date-related problem. Executive management understanding and support are required in developing year 2000 strategies because factors such as the magnitude, logistics, and complexity of the problem may serve as barriers at lower levels within the organization. We believe that, to foster appropriate corrective action, further steps are warranted to ensure that all levels of management within entities have a sufficient understanding of the problem and its associated risks.

> **To achieve a broader spectrum of awareness throughout the Commonwealth, we recommend that the Governor issue an executive order related to year 2000 compliance responsibilities and reporting requirements. The executive order should include additional requirements for centralized reporting for all state entities, and incorporate instructions similar to those outlined in Secretary for Administration and Finance Charles Baker's September 29, 1997 letter (see Appendix 4, page 74). The letter was sent to all executive branch secretaries and department heads regarding year 2000.**
>
> **To ensure that all entities become sufficiently aware of the year 2000 problem and how to address it, the Commonwealth should continue its efforts to provide year 2000 awareness seminars across the state. All reasonable efforts should be made to contact those entities that have not been confirmed as having assessed the impact of year 2000. Efforts should be focused on identifying**

and targeting entities that have not responded to the Fiscal Affairs Division's request for year 2000-related cost estimates, have not been interviewed by ITD's Y2K PMO, or have not attended year 2000-related meetings sponsored by ITD or the Department of Revenue.

To keep informed of what other parties are doing with regard to the year 2000 problem, entities should network with each other, consult with ITD's Project Management Office, attend Y2K user group meetings, and use Internet websites as an additional source (see Appendix 5, page 75), such as: Http://www.magnet.state.ma.us/y2k/ and Http://www.isaca.org/yr2000.htm

Assessment

The survey indicated that the majority of state entities had not adequately tackled the most important first step of assessing the impact of year 2000 and determining what needs to be done. Inadequate effort in this area will certainly result in year 2000 failures. The survey demonstrated that, except for few state entities, there were significant delays in completing assessments of the impact of year 2000 on information-systems-related technology.

At the time of the survey, 61% of those responding did not indicate that they had begun a year 2000 assessment. As a consequence, there were only a small number of entities that had formulated remedial action strategies or provided cost estimates for their year 2000 projects on the survey response. One cannot overlook that, without an understanding of impact and a clear picture of what needs to be done, we place at risk our abilities to rectify the situation. Adversely impacted are decisions regarding remedial actions, cost estimates and funding requests, acquisition of necessary resources, and implementation of corrective strategies.

The survey also indicated that where assessments had been performed, the process had been focused first on application systems; to a lesser degree on system interfaces, operating systems, security packages, and system software; and to a far lesser degree on all other technology. The heavier focus on application systems that support traditional business functions, rather than on other system software or technology-supported operations, or to the possible exclusion of other systems software or supporting systems (e.g., HVAC, security, utility-related software, etc.), is an approach not unlike other organizations addressing the year 2000 issue. Again, the comparison should provide little comfort, as there may be serious risks incurred by not adequately addressing these other vital areas of technology. To fully scope year 2000 projects and determine all required resources and costs, the assessment of impact of year 2000 must be made on all technologies as soon as possible.

A critical first step to performing an assessment is to determine exactly what software and technology comprise the IT environment. It is essential for agency or department administrators to have a complete and accurate inventory of their information systems and technology as part of an evaluation of the impact of their year 2000 problem. A high-level risk and exposure assessment and an evaluation of the criticality and importance of each application system should also be included. Once a corrective strategy has been formulated, it is the entity's responsibility to develop an appropriate project plan to guide the effort.

> **To ensure sufficiently comprehensive impact assessments, entities should assess the entire operational IT environment, including traditional and nontraditional business systems, equipment with embedded software across all platforms, and external systems supporting the entity's business functions.**
>
> **To ensure that year 2000 projects can be adequately planned; systems properly triaged; and realistic cost, resource, and time estimates developed; state entities must devote sufficient resources to complete their detailed year 2000 impact assessments as soon as possible. Entities not having adequate resources to complete their assessments and develop corrective strategies should contact ITD's Year 2000 Program Management Office for advice and assistance.**
>
> **To help ensure that appropriate controls can be designed and implemented over the IT environment, we recommend that a risk analysis of threats and exposures be performed on current systems and IT operations considering projected risks and exposures during the year 2000 project.**
>
> **As part of the assessment phase, we recommend that state entities prepare a complete inventory of printed stock where the date fields are preprinted with "19." A plan should be devised to allow this stock to run down by the turn of the century. Where heavy use is anticipated, a run of interim forms with no preprinted century should be considered for use before preprinted forms with "20."**
>
> **Based on the results of the assessment phase, we recommend that entities prepare and make available a statement of year 2000 impact on the citizens, other entities, and other recipients of state services provided by the entity's information technology. The statement of impact should also be used to guide the development of contingency plans.**

It is important that, during the assessment phase, entities determine the extent to which the values "99" and "00" have been used in date fields to signify something other than dates. Traditionally, "99" has been frequently used to represent "end of file," and the values "99" or "00" have been used to indicate that the file should be saved and never destroyed. Regarding year 2000, entities need to be aware of the existence of these identifiers within files so that corrections do not overwrite them and thereby destroy the instruction they were meant to provide. If not properly addressed, a number of adverse effects could occur. For example, a large number of files could be deleted on January 1, 1999 or 2000; applications may terminate upon encountering a record with a 1999 date, values with "99" or "00" could be ignored because the application system is designed to assume that they have a null value; or applications may continually attempt to read beyond the last record until encountering a value "99" (end of file). The "99" may have been changed to 1999, and therefore would not be recognized as "99." In other instances, 01/01/99 and/or 09/09/99 have been used to denote that the date of a particular data entry item is not known or has not been assigned. As a result, unexpected and undesired processing events associated with these practices could result on or after January 1, 1999. As a result, caution is needed to determine what the values represent and, consequently, what needs to be changed, since values represented by "99" may vary greatly among different systems.

To help ensure that important instructions are not lost during software fixes to date fields, entities should determine during assessment the extent to which the values "99" and "00" have been used in date fields to signify something other than dates.

Of the various corrective strategies, it may be feasible to use some form of workaround, such as windowing, to enable the system to process year 2000 dates. Windowing is a method used to avoid expanding date fields in non-compliant program code. Using windowing, certain assumptions about two-digit year dates are made within a translation program. For example,"00" through "20" may be assumed to be years in the 21st century, while "21" through "99" may be assumed to be dates in the 20th century. It is important to recognize that, because workarounds are to some degree "band-aids," which buy time for the entity's systems, the problem may need to be addressed in the future, depending on the system life cycle and on whether the workarounds continue to operate correctly. Although it is possible that the entity will have converted to an upgraded system by that time, plans for addressing outstanding workarounds should be in place.

To effectively manage subsequent date-related modifications in a timely manner, a complete inventory of workarounds with sufficient information should be maintained and cross-referenced to the entity's IT strategic plan.

Planning

As evidenced by a significantly small fraction of entities having formal year 2000 plans, adequate planning had not yet been performed to ensure that the Commonwealth's systems and technology will reach year 2000 compliance. Regardless of the size of an organization, or the extent or complexity of its technology, an entity's efforts to achieve year 2000 compliance requires careful strategic and tactical planning.

Although the survey indicated that certain entities had performed different levels of planning, only 14, or 5%, of the 282 entities that responded to the survey had written and approved year 2000 plans, and only 77, or 27%, of the responding entities had begun to plan their year 2000 strategies (see page 48). Ostensibly, only 77 were far enough along in the process to know whether they needed assistance. It is likely that the delays in completing the impact assessments had slowed the development of year 2000 plans. It is also evident from the survey that entities need to access outside resources to assist them in developing appropriate year 2000 strategies.

With respect to year 2000 planning, we have observed that there are some basic assumptions that could be erroneous. Listed below are some of the assumptions we believe are invalid and valid regarding year 2000 planning:

Invalid Assumptions

1. Year 2000 project planning and implementation is the sole responsibility of the information systems function.

2. Mission-critical systems reside only on mainframe computers.

3. Year 2000 compliance and business continuity planning validation is not needed for third-party information system vendors and business partners who have plans sufficient to achieve year 2000 compliance in time to meet the critical needs of your entity.

Valid Assumptions

1. Continued provision of critical and important services and operational survival into the next century should be recognized as primary goals of each entity.

2. The inability to maintain information systems operations for mission-critical systems beyond the time when year 2000 dates are used jeopardizes an entity's viability.

3. Year 2000 project planning must be carried out for the entire entity, not just the information systems department and should address all information systems and technology-supported operations.

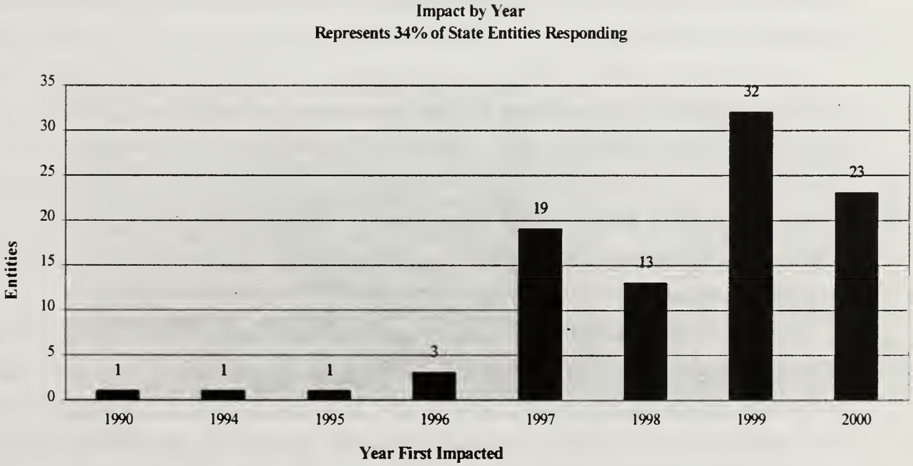
4. Timely funding for all resources required to carry out an entity's year 2000 project must be a priority and budgeted as a cost of maintaining operational viability.

5. Year 2000 testing and validation methods should always be performed for all systems and technology.

From a planning perspective, we are concerned with the consequences of the year 2000 problem that may impact entities much earlier than assumed by some of those who have not completed their impact assessments.

Essentially, the impact threshold may be earlier, should the system require the use of a year 2000-related date before January 1, 2000. State entities, such as the Registry of Motor Vehicles and the Department of Transportation have already been impacted by year 2000 dates. It is imperative, therefore, that assessments be completed as soon as possible to identify critical-event horizons of the year 2000 impact and to plan for remedial action and/or contingencies.

Our survey indicated that only 15% of all state entities, or 34% of those responding to the survey, could identify when their systems would first be impacted by the year 2000 problem (see graph below). Of those that did respond, 38 projected being impacted before 1999, and 32 estimated their first impact to occur in 1999,and 23 entities would be first impacted in the year 2000.



Impact by Year
Represents 34% of State Entities Responding

Figure 3

Although Figure 3, above, is based on a limited number of responses, the year 1999 may be the point at which many entities are first affected by the year 2000 issue. In certain instances, the date problem may occur when using 1999-related dates in the event that the system uses the value "99" in the date field to represent something other than 1999 (see discussion of this issue on pages 15 and 16).

Another example of a system which has a date-related problem is the Geographic Positioning System (GPS) rollover, which will occur at 00:00:00 UTC, August 22, 1999. GPS uses its own clock, based on a predetermined and limited number of cycles that require periodic rollovers. Inaccurate date and time values and incorrect coordinates may result if GPS receivers have not been prepared for this rollover.

In the course of modifying systems to be ready for year 2000, entities will also need to ensure that the systems can correctly process with regard to the leap year, the date variation of which occurs two months after January 1, 2000. In this case, the systems will need to properly recognize year 2000 to enable correct processing with respect to leap-year logic.

As we have noted, the planning for remediation must address all information technology. To ensure continued operations, decisions regarding corrective strategies must include all critical and important software, hardware, firmware, microcode, operating systems, application systems, job control language, software compilers, queries, procedures, calls to other programs, screens, databases, and data. Entities should avail themselves of technology resources, such as software products designed to locate date fields and to simulate what will happen after December 31, 1999. If not already completed, planning regarding system change prioritization and required resources such as additional staff, analytical software, and outside assistance should be performed as soon as possible.

Understandably, the nature and extent of the year 2000 impact, available resources, expected completion timetables, and cost will affect an entity's strategy. With regard to the strategy to be used in remediating date fields, the survey indicated (question No. 8 under "Planning," in Appendix 1), with 94 responses, that a strategy of converting all two-digit date fields to four digits had the highest ranking. The second highest ranking for the question was 86 responses, indicating that entities were relying on package vendors to provide the solutions. Significantly smaller numbers responded that strategies would include bridge programs or piecemeal developments.

There are very real benefits to benchmarking to obtain the "best practices" with respect to what other organizations are doing to address year 2000 compliance. However, entities should focus on what practices have led to successful year 2000 projects, rather than merely comparing where one is in relation to everyone else. The latter may cloud perception of where the entity's systems and technology need to be with respect to year 2000 processing capability.

In the development of strategic and tactical plans, we suggest that entities consider establishing the priority of information systems and supporting technology based on the level of mission-criticality, level of risk of malfunction, potential exposure from failure to operate as intended, and complexity of achieving year 2000 compliance. Entities should establish software configuration management techniques consistent with the size and complexity of their IT environment. If software is to be used to perform this function, it should be implemented at the beginning of the year 2000 project (or earlier), and staff should be trained to use it upon its implementation or as soon as possible. With respect to acquisition, procurement procedures should require that all equipment, containing embedded software or firmware that is impacted by dates be year 2000 compliant. Furthermore, until year 2000 compliance has been attained, the entity may consider leasing equipment to provide increased flexibility in upgrading and reallocating IT resources. Regarding implementation, entities should establish control procedures to ensure that future software development and maintenance complies with year 2000 requirements. And, considering the importance of system availability, entities may need to strengthen backup procedures for on-site and off-site storage of backup media and determine whether more aggressive backup schedules and new requirements for archival copies of backup media are warranted. If possible, dual control should be exercised over off-site backup copies for all mission-critical and important systems.

As part of the overall strategy, entities should determine whether to develop or enhance their own technical resources to address assessment, conversion, testing, and implementation. If such technical resources are unavailable, then outsourcing decisions need to be made. Entities also need to develop year 2000 methodologies which include adequate user review and approval, targeted completion dates, business continuity planning, and controls to prevent and detect the inadvertent reintroduction of date-related problems.

To help ensure that required resources will be obtained in a timely manner, that costs will not be increased due to lost opportunities, and that required contingency plans will be developed for systems that may not be ready in time, state entities should complete their detailed year 2000 project plans for their entire IT environments as soon as possible.

To assist in developing year 2000 project plans, entities should benchmark against those remediation practices that have led to successful year 2000 projects, incorporating them when appropriate within their own projects.

To help ensure that year 2000 efforts are properly directed, entities should prioritize systems based on their level of mission-criticality, level of risk of malfunction, potential exposure from non-compliance, and complexity of achieving year 2000 compliance. Management should consider focusing compliance efforts on mission-critical systems; evaluating the consequences of noncompliance for less critical systems; and developing appropriate contingency plans to address needed services.

Entities supporting complex and/or multiple software systems should assess the need for using software configuration management techniques. If software is to be used to perform or manage this function, it should be implemented at the beginning of the year 2000 project (or earlier), and staff should be trained in its use upon its implementation or as soon as possible.

With respect to date processing objectives, entities should ensure that the systems can process correctly with regard to the leap year, the date variation of which occurs two months after January 1, 2000.

ITD should integrate year-2000 requirements within standards and guidelines issued by the Commonwealth's Committee on Information Technology Standards and Guidelines.

Entities should adopt contract and warranty language developed by the Operational Services Division (OSD) of the Executive Office for Administration and Finance. We recommend that year 2000 contractors be bonded.

To ensure that entity systems can operate in concert with third-party provider systems, sufficient assurances should be obtained that stated plans are being adhered to for year 2000 compliance, that date field formatting is synchronized with entity systems, or that conversion programs are developed in time. Entities should obtain sufficient evidence of year 2000 compliance and business continuity planning validation for third-party information system vendors and business partners to meet the critical needs of the entity.

We recommend that entities consider leasing equipment to provide increased flexibility in upgrading and shifting IT resources, if required equipment has not yet achieved year 2000 compliance.

Entities should identify all printed stock of forms that are pre-printed with "19" in the year fields and plan for a "safe" shift to the year 2000 format by allowing current stock to run down and reorder modified stock in time to change to the 2000 format.

Entities should send a representative to ITD's Year 2000 User Group meetings.

Until such time as year 2000 compliance is fully attained, information technology acquisition and development initiatives must address year 2000 compliance.

To expedite corrective efforts, year 2000 project plans should identify as soon as possible the priority of required changes and resources, such as additional staff, analytical software, hardware, and third-party assistance.

Given that important systems need to achieve year 2000 compliance, we recommend that management consider setting aside less essential IT-related projects where resources could be reallocated to year 2000 projects. In that light, we recommend that ITD identify ongoing IT projects that are non-mission critical or not mandated by law where associated resources could be reallocated to year 2000 projects. If required, the Governor should consider postponing IT projects not mandated by law in order to free resources for year 2000.

To ensure that the integrity and security of systems and data are maintained, appropriate internal controls must be in effect throughout all phases of year 2000 projects. Especially important, are controls to protect systems and data from unauthorized access and change and to ensure that modifications are reviewed, tested, and approved before being migrated from the test environment into production. Given that persons from outside the entity may be required to have access to systems and data files during assessment and reprogramming, existing security methods may need to be strengthened to address security and operational control objectives. We recommend that state entities require that procurement of all software, hardware, and equipment containing embedded software complies with the requirements of year 2000.

Incorporated within the fabric of each entity's internal control structure should be control objectives and controls to ensure system and data integrity is maintained with respect to year 2000 compliance. Appropriate procedures should be implemented to ensure that program change controls and program version controls are in place at all times throughout the year 2000 project. We further recommend that entities establish control procedures to ensure that future development and software maintenance attains year 2000 compliance.

We recommend that each entity establish appropriate monitoring controls to track, evaluate, and report on the progress of year 2000 initiatives including the quality of year 2000-related software changes and the viability of modified systems and technology.

We recommend that entities address year 2000 compliance in cooperation with other entities by networking and taking advantage of resources inside and outside of state government.

To ensure that parties who depend on the entity's systems are aware of year 2000 status, the entity should establish a cost/effective manner to keep all relevant parties informed of year 2000 initiatives.

We recommend that the State Treasurer take all prudent steps required to protect the state's private sector equity investments, given the expected disruptions in the publicly-traded equity markets that may be caused by the year 2000 problem.

Responsibilities and Accountability

The current framework of accountability for ensuring that IT systems are year 2000 compliant appears to reside solely with the entity in which the system resides. We believe that there are two potential problems with this premise: first is the issue of to whom the responsibility has been assigned within the entity, and second is the issue of whether the entity itself is sufficiently empowered to carry out the responsibility.

Regarding the first concern, the survey indicated that, in many instances, the individuals assigned responsibility for addressing year 2000 compliance were the MIS or IT directors. Clearly, while IT management has a significant role to play regarding year 2000, not all systems may be within their responsibility. Now, important computer systems and IT resources can be found across and within different organizational boundaries. The pervasive nature of technology has placed various IT operations outside of the traditional IT departments. Under such circumstances, it is possible that adequate attention may not be afforded to certain systems or technology not residing under the organizational control of the MIS director. In such operating environments, because of the critical importance of year 2000 compliance to the entity, final responsibility should be assigned at a senior executive level.

The second concern is that the entity itself may not be sufficiently empowered to ensure success. The assignment of final responsibility may not be appropriate in those situations where enterprise-wide decisions (e.g., across a secretariat, or entity having multiple departments), rather than per entity, need to be made, or where those entities deemed responsible have an almost impossible task before them to obtain the resources needed to assess, plan, and implement year 2000 solutions. And as a related matter, the entity-specific assignment of responsibility affects decisions made, or not made, regarding what systems get modified. Where appropriate, secretariat level reviews should be made of decisions made by individual entities.

From an organizational perspective, regardless of whether certain technical services are outsourced, responsibilities must be assigned to perform the required technical services and provide management oversight and approval. In addition, entities need to consider establishing project teams to address year 2000.

> **We recommend that year 2000 be addressed with an enterprise-wide perspective and that the responsibility for year 2000 compliance be assigned to a senior executive or a level of management sufficiently high within the entity to ensure that the project can be accomplished in a timely manner.**
>
> **To ensure that adequate attention and resources are applied to the year 2000 problem, entities should establish a year 2000 project team comprised of members who are adequately trained, possess sufficient technical knowledge, and have strong communications skills. To ensure that senior management is kept fully aware of key year 2000 issues and problem resolution, the year 2000 project leader should have direct access to senior management.**
>
> **To oversee and guide the entity's entire year 2000 project effort, year 2000 steering committees should be established at the entity and secretariat levels. At the entity level, the steering committee should be chaired by a member of senior management, have representation from key user departments, and should include the year 2000 project leader. The year 2000 project-team leader should report to the steering committee for review, approval, and oversight of project**

activities. At the secretariat level, the steering committee should also be chaired by a member of senior management and have adequate representation of entities within the secretariat.

It is our observation that ITD's Strategic Planning Group, through its establishment of the Y2K Program Management Office, has developed an excellent resource for year 2000 planning for the Commonwealth and individual state entities. While this operation should have been established quite some time ago, the Y2K Program Management Office has made substantial progress since the group's inception in June of 1997 and is available to assist other entities in addressing year 2000 compliance. However, not unlike many enterprises, the Commonwealth does not have sufficient expertise internally to adequately assess the impact of year 2000 and to provide workable solutions. In addition, it may be very difficult to secure adequate resources for year 2000 projects. Therefore, state entities need to proceed as quickly as possible on year 2000 compliance matters and use all available resources at their disposal.

The ability to engage sufficient third-party assistance may be jeopardized by the market itself, as private-sector and other entities external to the Commonwealth may be able to outbid the state in contracting for needed services. Furthermore, given time and resource constraints, entities may need to make some difficult decisions regarding what systems will attain year 2000 compliance, what IT projects will need to be delayed, and what efforts will need to be directed toward developing workable contingency plans. Although there is a general understanding of the year 2000 issue, until the detailed assessments are completed, it appears that the level of understanding throughout the state will be insufficient to make the difficult decisions necessary in allocating limited resources to year 2000 projects.

Cost

At the time of the survey, the total cost of achieving year 2000 compliance for mission-critical and important systems was unknown. As of the issuance date of this report, cost estimates for the Commonwealth have ranged from $50 to $70 million. A more accurate cost estimate cannot be provided at this time because not all impact assessments or remedial plans have been completed, nor have problems been identified through testing. While the Executive Office for Administration and Finance's (EOAF) Fiscal Affairs Division and ITD are making a good-faith effort to identify total costs, accurate estimates must be established for each entity. Understandably, the effort may be impeded by the absence of adequate assessments by certain state entities.

With respect to total cost, total estimates presented through our survey are significantly higher than amounts previously stated by senior officials. Although the $70 million total cost brought forward through the survey may be subject to error, this initial effort to determine state-wide costs reflects some of the difficulties in determining exactly what should be counted as part of the year 2000 effort and as part of estimating total cost. We expect, however, that as entities complete their assessments on all technology, and develop corrective plans, more accurate figures will become available.

Entities should work closely with ITD's Y2K Program Management Office and with the Fiscal Affairs Division to establish year 2000 funding requirements before it is too late. As of December 1997, only 61 agencies had reported their funding needs to the Fiscal Affairs Division.

Year 2000 project teams within entities should work closely with their entity's fiscal management to keep them informed of changes in cost estimates as individual projects progress.

Contingency Plans

Currently, the Commonwealth at large has not developed sufficient contingency plans to ensure continuity of critical and important services should automated systems fail to operate correctly, or at all, when processing Year 2000 dates and dates beyond. Given the current status of year 2000 efforts and that sufficient, comprehensive testing has yet to be performed to identify difficulties that are anticipated to be discovered through testing, it is likely that certain systems will not attain year 2000 compliance in time and that alternative processing methods will be needed.

To help ensure viable operations and protect services, entities should establish contingency plans for all systems for which there is either a likelihood that the systems will not attain year 2000 compliance, or for systems not to be made year 2000 compliant in time.

We recommend that entities strengthen backup procedures for on-site and off-site storage of backup media; determine whether a more aggressive backup schedule is warranted; and exercise dual control over off-site backup copies for all mission-critical and important systems.

System Modification

Given the delays in assessing impact and developing corrective strategies, it is not surprising that a majority of the entities responding (approximately 93%) indicated that their information systems did not meet the requirements for year 2000 compliance at the time of our review. Only 21 entities (7%, of those responding or 3.2% of all entities) indicated that their software was in year 2000 compliance at that time. Even if better information were available as to which systems and technologies needed to attain year 2000 compliance, it is likely that a substantial portion of information technology would be indicated as non-compliant. Clearly, what is important at this point is to specifically determine what needs to be modified, closely monitor the status of conversion efforts, and exercise good internal controls over this process.

It is during the system modification phase that entities actually make the changes to their application systems, whether converting code, building window or bridge code to temporarily defer the year 2000 problem, eliminating code, building workarounds, or replacing hardware and software. Programming changes should be carried out by in-house and/or vendor programmers, consistent with the solution designed in the assessment and planning phases. In all instances, it will be important to consider the complex interdependencies among systems and applications, whether in-house or through external entities. During this phase, and subsequently, management must ensure that adequate project management is in place and that internal control is maintained over system and data security, confidentiality, and all program changes and versions. Our survey indicated that 54, or 19%, of the 282 responding entities were not documenting all code and system modifications. This is a serious control weakness. In all future year-2000 remediation efforts, it is imperative that each software change be properly documented.

> **Legislative initiatives resulting in mandated changes to automated systems should take into consideration the impact on critical year 2000 projects along with the assessment of other usual factors such as cost/benefit, technical feasibility, security, and business continuity planning. Management initiatives, as well, should also assess the impact on year 2000 projects.**
>
> **Remedial action should be triaged so that the most critical business critical systems attain year 2000 compliance first. To the extent possible, remedial action of various mission-critical systems should be carried out in tandem, and test scripts and test databases should be built as the remedial action process is carried out.**

The year 2000 issue is a managerial problem, best solved by strong project management techniques. Although at first glance, correcting the year 2000 problem may appear to be a relatively simple, technical problem ("after all, programmers need only to add two fields to date formats") it may present a daunting project management challenge. The project management skills required include in addition to planning, organizing, staffing, directing, and coordinating, clearly defined projects with specific deliverables, clearly-defined points of accountability, monitoring and status reporting.

Some systems contain millions of lines of program code, with large numbers of date fields, the purpose and impact of which may not be immediately apparent to the programmer or to the software product used to identify or implement the code change. The need to "parse," or segment, systems and programs so that several programmers can be working simultaneously on different subsystems, modules, or code segments will, most probably, becomes imperative. When the program code is reassembled, all the modules or pieces must function together and the entire system must perform as intended on its own and in conjunction with other systems. At the same time, the original object code has to be kept in production, and unrelated changes may need to be made to the production copy. Any such changes need to comply with the requirements of year 2000 and be brought forward into the corrected code.

Software and technology conversion efforts are already proceeding under extremely tight time constraints. Time is of the essence. Under such circumstances, the application of strong project management techniques is pivotal, if we are to avoid costly mistakes that consume precious time and jeopardize a successful outcome. Experience has demonstrated that in environments where multiple tasks are occurring simultaneously, management control techniques, such as the establishment of a year 2000 master plan, formal conversion plans to address application and operating system functions, the use of PERT and GANTT charts, program change control techniques, and program version controls are essential.

Regarding the year 2000 planning efforts, it is necessary that entities ensure that there are adequate controls in place for the ongoing review and update of the master plan as the project moves forward. Management will need to put in place a methodology to anticipate when resource levels greater than those expected will be required. In addition, it is essential that entities keep track of the entire project, applying feedback and lessons learned inside and outside of the project to future project areas.

To guide and monitor their year 2000 projects, we strongly recommend that entities use project management techniques.

To ensure that an entity's year 2000 project is given adequate direction, careful consideration must be given to the skills required to manage the project when selecting and appointing the project-team leader. Staff currently in charge of operations should not be expected to lead the year 2000 project, while also carrying out day-to-day duties.

When windowing is to be used, entities need to ensure that year 2000 assignment assumptions used are in sync with other systems, be they internal or external to the entity.

Program Change Control

The failure of entities to exercise an appropriate level of controls over the process of modifying systems for year 2000 could result in systems that fail to function as intended, or at all, or in systems that produce erroneous results that could remain undetected for an extended period of time. As with any program change process, it is necessary that controls be in effect to ensure that source and object code are kept in sync. It is also advisable that management ensure that there are adequate backup copies of mission-critical data files and programs for all platforms prior to year 2000 remedial actions. The backup copies will serve as documentation of electronic files prior to year 2000 modification, and, as stated earlier, many original programs may be useful to run archival reports in the future, if archival data is too extensive to convert.

> **To ensure consistency in making year 2000 required program-code changes, to provide a means of control, and to provide an audit trail of what was changed, when, and by whom, we recommend that program-change-control software be used on all year 2000 projects that are deemed to be of sufficient complexity.**
>
> **To ensure that entities can recover from possible errors that may render that code unusable, we recommend that entities maintain full backup copies of files and systems prior to remedial activities.**
>
> **We recommend that state entities establish control procedures to ensure that future development and software maintenance is year 2000 compliant.**

Data Management

As systems are modified to attain year 2000 compliance, entities may need to access prior data that has been stored in electronic form. Here, the entities will need to address backward compatibility in order to access unmodified existing data and archival data. Entities must plan, if they are to retrieve archival data. Some archival data may be converted to year 2000 compliant formats; however, other data files may not be converted due to volume or other reasons. Backward compatibility may require that original program versions and those programs that have attained compliance are maintained and available to process converted and/or non-converted data for a prescribed period of time. In other circumstances, data files that are not to be converted to a year 2000 compliant format may be accessed using bridge programs to read the data.

> **To allow access and processing of existing and archival data, we recommend that entities plan for either conversion of such data, or the provision of an alternate means of processing such data.**

System Access Security

Regarding system access security, it is recommended that management review access security policies and procedures to determine whether current controls are appropriate. Managers must ensure that individual accountability is enforced. In most environments, there will be a need to sufficiently prohibit unauthorized access and to document all access and actions taken. Because outside contractors may be engaged, managers need to ensure that access privileges for contracted third-party staff are promptly deactivated when the contracted parties are no longer authorized to have access, or upon their termination from the projects or contracts. For some application systems, the issue of confidentiality of sensitive data may require that special precautions be in effect to ensure that data files are adequately protected during the data conversion phases of the year 2000 project and to ensure that all backup copies are comparably protected.

> **We recommend that management review access security policies and procedures to determine whether current controls are appropriate.**
>
> **To ensure accountability, we recommend that managers ensure that individual accountability is enforced and that unauthorized access to year 2000 programs and data is specifically prohibited.**
>
> **To maintain the integrity and the required level of security over production libraries, entities should have adequate controls in place to protect on-line and archival data files from unauthorized access and modification.**
>
> **When making year 2000 modifications, especially when third-party vendors are to be engaged, controls must be established and exercised to protect confidential and sensitive data from unauthorized access.**

Documentation

Documentation is one of the fundamental components of internal control, along with systemization and competent and trustworthy personnel. Not only is the documentation of the entire system necessary (overview to detailed specifications), but adequate management trails of changes to the systems must be in place in order to permit their review and allow for corrective action, if needed. Clearly, documentation is vital for a variety of purposes, including the updating of program code, user manuals, and training materials. Data input screens may need to be modified to allow users to input the two-digit century designation and reports may need to be changed to reflect the century designation. It is essential that documentation be appropriately updated as the project moves forward, or as soon thereafter as is possible. Programmers and others working on the year 2000 project must be required to maintain detailed documentation on all year 2000 activities. Failure to adequately document year 2000-related system changes and related user documentation may result in costly and time-consuming errors in the future.

Testing

Our survey indicated that very few entities were at the stage of conducting tests on program code that has been modified for year 2000. Only 22, or 8%, of the 282 entities responding had developed test and validation plans, only 7, or 2% had implemented automated test tools, and only 18, or 6%, had implemented acceptance testing.

Units of application programs and/or subsystems should be tested for full operational year 2000 compliance as soon as programming modifications for each unit is completed. During unit, system, and integration testing, the test environments should provide access security controls appropriate to the systems and data being tested. Each complete system, including all units and/or subsystems, should be tested for full operational year 2000 compliance as soon as the modifications are completed for the entire system. Upon the completion of year 2000 compliance modifications required for all systems, the systems should be tested. This phase should include user verification of year 2000 compliance and user acceptance tests.

To ensure the adequacy of testing, we recommend that entities develop and document test and validation plans for each converted or replaced application of system component, and should implement automated test tools and scripts as appropriate to the automated system being made year 2000 compliant.

Entities with large, complex systems should establish a specialized testing and compliance team, with required skill sets, and implement a year 2000-test facility.

Entities should develop and document a strategy for testing contractor-converted or replaced applications or system components.

To ensure uniformity of compliance results, entities should perform unit, system, and integration tests on each converted or replaced system and system component.

Testing should include regression, performance, stress, and forward and backward test procedures, as appropriate.

Entities should track the testing and validation process and collect and use project-related statistics to manage it.

We recommend that entities incorporate user acceptance testing.

We recommend that, in all cases, entities successfully complete acceptance testing prior to the introduction of new software to the production environment and that entities reintegrate the

converted and replaced systems and related data with the new software in as timely a manner as is possible.

Implementation of Remediated Software

After remediated software has been successfully tested and accepted by management and users, the modified systems would be reintroduced to the production environment. It is important that, from that time forward, all input of data containing year fields, including those from outside the entity, conforms to the new year field standard, e.g., CCYY. State entities operate many systems that provide data flows to and from other state systems, federal systems, and private sector systems, see Figure 4.

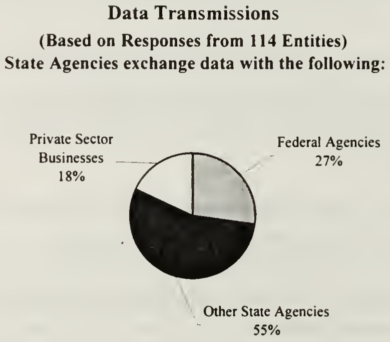


Figure 4

As systems are reintroduced within the production environment, careful consideration should be given to the interrelationships of systems, whether internal or external to the entity, so that data flows between systems remain in sync with regard to date fields. Systems should be brought back into production as soon as possible, after testing has been successfully completed. In this regard, temporary bridge programs may be required, as remediated systems are required to operate with those that are not yet remediated. In other instances, windowing may be required. When using windowing, care must be taken to keep data communications in sync when windows with different assumptions are involved.

To expedite the implementation of remediated software, we recommend that entities define their transition environment and procedures, develop and document a schedule for the implementation of all converted or replaced applications and system components, and resolve all data exchange issues and interagency concerns.

To avoid problems when systems made compliant are reintegrated, we recommend that date field formatting be synchronized, or conversion programs established, for data interchanges with third-party information systems vendors and business partners.

Entities should assess the degree to which software tools can be used to prevent and detect importing incompatible date-formatted data.

To ensure proper implementation of remediated software and systems, we recommend that the year 2000 testing and compliance team be assigned the responsibility of validating and certifying test results, providing assurance that the remediated software operates as intended when reintroduced to the production environment, and ensuring that such software functions properly with all internal and external interfaces.

We recommend that entities expedite database and archive conversions, as appropriate.

When modified software is reintroduced to the production environment, we further recommend that entities develop associated contingency plans and update or develop disaster recovery and business continuity plans.

Reporting

It is important that entities establish a formal, centralized reporting system for year 2000 project status, and require submittal of exception reporting to senior management for review. In addition, special attention should be given to year 2000 compliance efforts for the Commonwealth's mission-critical systems that are significantly delayed.

We recommend that a system of centralized reporting of year 2000 project deliverables (e.g., correctly modified system code) be developed and implemented state-wide. Compliance status and validation of corrective action should be established and reported to track progress of individual entities and the Commonwealth at large.

Entities should keep their client base informed as to what actions have been taken to ensure year 2000 compliance for systems (and subsequent status), especially when those clients are dependent upon the entity's systems.

Legal Issues

There are enormous legal implications regarding the year 2000 issue. Some legal experts have predicted that year 2000 noncompliance cases will comprise the single largest litigation expense in history, incurring legal costs that could surpass $1 trillion. Beyond the interdependencies forged through electronic transfer of data and electronic commerce are the expectations of delivery of service, safeguarding the integrity of information held in trust, and safeguarding assets that may be at risk should litigation result from systems or technology that fail because they are not year 2000 compliant.

It is a primary responsibility of management to perform strategic planning sufficient to ensure that an entity's mission can be carried out, that mission-critical systems will operate as intended, and that the information and data those systems generate will have integrity. Management responsibilities include having in place internal controls to provide reasonable assurance that operational objectives will be achieved and that undesired events will be prevented or detected and corrected. In carrying out its planning and operational obligations, management must exercise due care, or in some cases due professional care. To steer clear of charges of negligence, or to defend against such charges, management should be able to demonstrate that it exercised due care. We believe that with respect to year 2000, entities should be able to demonstrate that they adequately assessed their entire information technology environment and, at a minimum, made a good faith effort to implement corrective strategies for essential systems and technology. That good faith effort should include informing users of systems and or trading partners of the status of year 2000 compliance. Clearly, the issue of demonstrable due-professional care will become increasingly important if systems fail to operate properly, or at all, because of the year 2000 problem.

The Operational Services Division (OSD) of the EOAF has developed and implemented a policy of requiring vendors which are to be listed on the state's "blanket contract" to sign a year 2000 compliance statement. The year 2000 compliance statement stipulates that all goods and services delivered by the signatory vendor must comply with the requirements of year 2000, imposes certain penalties, and indemnifies the state for breaches in goods and services delivered under said contracts, resulting from year 2000 noncompliance.

Care must be taken to ensure that copyrights are not violated and that proprietary information is appropriately protected against unauthorized access, use, and/or disclosure. If an entity does not own the software product it is using, it should not be modified for year 2000 unless the license agreement allows for such modification. When there is a question regarding copyright issues, management should consult the software vendor.

Entities occasionally have agreements with third-party software providers whereby the application program's source code is held in escrow as a protection against the vendor going out of business or otherwise defaulting on contractual agreements. When program code is held in escrow, the vendor would be required to modify the software for year 2000 compliance as part of the software license agreement; however, entities need to ensure that the escrowed copy of the source code is updated in accordance with the compliant version.

Our survey indicated that 86, or 31%, of those state entities responding are dependent upon and are awaiting vendor solutions promised by software vendors. Many entities are also awaiting vendor-promised "fixes" for year 2000 hardware compliance. In some instances, it is expected that vendors will be unable to deliver promised "fixes," and others may go out of business rather than suffer costly litigation. In such cases, the responsibility for year 2000 compliance is made more complex, but remains with the entity's management. Nonetheless, the danger for entities in this situation is that by the time they become aware of the problem, the opportunity to achieve year 2000 compliance may have expired. Documentation of vendor-promised solutions and the provision of adequate business continuity planning take on heightened importance in these situations.

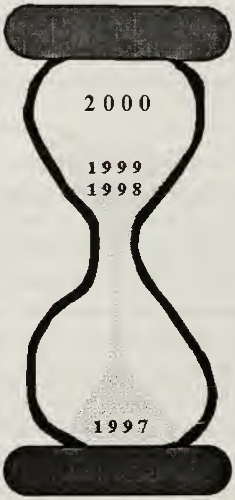
Entities should maintain complete documentation of efforts to assess year 2000 impact including the development of strategies and tactical plans for addressing the issue, and taking remedial action, verifying test results, implementing modifications and technology, informing parties as to year 2000 actions, and assessing the status of information systems and technology. We also recommend that entities maintain careful records of all activities involved in their year 2000 project. This would include, but not be limited to, the year 2000 planning documents, year 2000 steering committee meeting minutes, documentation of decisions regarding mission criticality and importance of affected systems and associated triage decisions, resource and cost estimates and methods of projecting them, project status reports with timelines and milestones, year 2000 project staff organization, staff qualifications, and training provided regarding year 2000 remediation.

The Governor and the Legislature should consult with the Attorney General in considering possible legislation to limit the Commonwealth's liability arising from year 2000-related occurrences.

We recommend that agencies contract only with those vendors that have signed the year 2000 blanket contract language as developed by the Operational Services Division (OSD). Agencies should be aware that OSD has written standard year 2000 contract clauses for contractual agreements, and entities should use these clauses in all new requests for response (RFRs) and contracts.

We recommend that entities perform a potential liability self-assessment with regard to year 2000 noncompliance and begin now to protect against the occurrence of these liabilities

Where software source code is being held in escrow, entities need to ensure that the escrowed copy of the source code is updated to the version that has attained year 2000 compliance.



Appendix 1

Survey Responses

The OSA mailed or, in another manner, distributed 607 survey questionnaires to state agency heads. In addition, the survey was included as part of an ITD Y2K publication and recipients were asked to complete the survey and send it to the OSA; 31 surveys were received in this manner. We determined that of the total 638 surveys in the population, 434 were represented in the final responses. As a percentage, 68% of the total population of agencies were represented, while 32% failed to respond in any way. What is somewhat troubling in these numbers is not only that almost 1/3 of surveyed agencies failed to respond, but also of those who did, only 86 agencies responded by the due date of May 16, 1997 (see Figure 1) on page 10.

In attempting to obtain a better result, in June 1997, the OSA began a schedule of telephone calls to agencies that had failed to respond. During the period June through August 1997, three calling schedules were carried out, contacting agencies that had failed to respond. Still, responses were slow to be received. Surveys continued to be received over that period and beyond, with a final cut-off date set at October 7, 1997. The OSA decided to use October 7, 1997 as a final cut off date to allow respondents a maximum window of opportunity before generating survey results, and to issue this report based on responses received as of that time.

Regarding completed surveys, we noted that a total of 282 surveys were returned to the OSA. Of this number, 251 originated as mailed surveys, and 31 originated as surveys from the ITD publication. Because certain agencies had their data processing provided by a centralized function at a higher organizational level, certain completed surveys were submitted and were deemed to represent multiple responses. We found that an additional 152 agencies were represented in this manner.

In summary, we believe that the slow rate of response and, in some instances, a failure to respond can be viewed as supportive of our overall conclusion that the Commonwealth as a whole is not sufficiently informed regarding the Year 2000 problem, and has not yet effected programs to obviate it.

The Commonwealth of Massachusetts

AUDITOR OF THE COMMONWEALTH

ONE ASHBURTON PLACE, ROOM 1819
BOSTON, MASSACHUSETTS 02108

TEL (617) 727-6200

A. JOSEPH DENUCCI
AUDITOR

97-7055-4W

As of October 7, 1997

Year 2000 Survey Results

The Office of the State Auditor is conducting a survey on the Year 2000 issue. The purpose of the survey is twofold. First, it is designed to identify the extent to which agencies of the Commonwealth have assessed the impact of Year 2000 on their automated systems and to determine the extent to which mission critical information technology has been, or will be, made Year 2000 compliant. Second, the survey was developed so as to serve as a high-level checklist for agencies in reviewing their status with respect to the Year 2000 issue.

Note that the survey may also be found on the Intranet at (**http://www.eoaf.state.ma.us**). The information obtained from surveyed agencies will be summarized by our Office and the Information Technology Department. Given the immediacy of the Year 2000 issue, we would greatly appreciate it if the survey could be completed as soon as possible and either mailed to our Office at the above address, to the attention of Robert Buchanan, or e-mailed to (Robert.Buchanan@SAO.state.ma.us) no later than **May 16, 1997**. Understandably, unless your agency has already performed a detailed self-assessment regarding the Year 2000 problem, it is possible that answers to some of the questions will not be known.

If you have any questions regarding the survey questionnaire, please contact:

Bob Buchanan	(617) 727-6200, ext. 173 e-mail: (Robert.Buchanan@SAO.state.ma.us)
Joyce Blackman	(617) 727-8638 e-mail: (Joyce.Blackman@SAO.state.ma.us)

Thank you in advance for your assistance.

Agency/Authority/Department/Division's

Name Phone Number

Organization ____________________ ____________

Department Head ____________________ ____________

Information Systems Officer ____________________ ____________

Year 2000 Manager ____________________ ____________

Survey completed by ____________________ ____________

I. Awareness

1. Is your agency aware that with the arrival of the Year 2000 most software and technology using date fields for calculations or other processing will be unable to process these date sensitive transactions correctly after December 31, 1999?

Yes		No		Blank	
	228		**9**		**45**
	81%		**3%**		**16%**

Auditor's Comment: The above figures indicate that a relatively high portion of those responding to the survey were aware of the Y2K issue. However, considering that 32% of those surveyed did not respond and that 19% of those responding either indicated "no" or left the question blank, we believe that this represents a sizable number of entities not sufficiently aware of the Y2K problem, thereby placing any necessary remedial actions at risk. By the time of the survey, every entity should have been aware of the Y2K problem.

2. Has management set an organizational goal to have business operations ready for Year 2000 before any disruption caused by 2-digit-year data occurs?

Yes		No		Blank	
	143		**89**		**50**
	51%		**32%**		**17%**

Auditor's Comment: As the figures indicate, slightly more than half of the entities responding had set an organizational goal to have business operations ready for year 2000. These results are less than encouraging considering that almost half of those responding had not set this goal.

3. Has your agency begun an effort to ensure that your information systems are Year 2000 compliant?

Yes		No		Blank	
	164		**71**		**47**
	58%		**25%**		**17%**

Auditor's Comment: The figures indicate that almost 60% of those responding had initiated efforts to become Y2K compliant. By combining the "no" answers with those left blank, we compute that slightly over 42% of the entities responding had not begun any efforts to address Y2K compliance. While the figures indicate that efforts were underway for a large portion of entities, the failure of remaining entities to take constructive steps may place their systems at risk of not being Y2K compliant in time.

4. The current status of your Year 2000 initiative is: (Please select all that apply.)

60	None planned	**45**	Repair
72	Planned	**42**	Test & validation
50	Inventory	**20**	Completed
82	Assessment	**28**	Other (Specify)

Auditor's Comment: Although responses may be given for more than one category or phase by the same entity, in total they indicate that the majority of those responding were in the earlier phases (planning, inventorying, and assessment) or had yet to begin. The results indicated that a smaller number of agencies were in the latter categories (repair, test and validation) and that only 20 entities had completed Y2K projects. Of the 28 entities that provided an answer to "other," the majority indicated that they were purchasing new software or equipment.

5. Is your agency on schedule to assess the impact of Year 2000 on information technology and to take corrective action if necessary? (Please select one)

46	Blank
38	N / A
101	No schedule established
71	On schedule
7	Ahead of schedule
4	Behind schedule, < 3 months
1	Behind schedule, 3-6 months
0	Behind schedule, > 6 months

Auditor's Comment: Although the figures indicate that some progress was underway on conducting impact assessments, it is somewhat worrisome that 35% of those responding had not established an assessment schedule. Considering that only 16% of the entities responding indicated that they had completed a Y2K assessment (reference: question 2, section II), it appears that, overall, the state is significantly behind schedule. All entities should have completed their Y2K assessments by the time of the survey.

6. Who at your agency has overall responsibility for the year 2000 issue?

178 responses were provided. Included responses indicated that, in many instances, responsibility had been assigned to the director of an entity's MIS or IT department.

Auditor's Comment: Considering the relative importance of the Y2K problem and that, in many instances information technology resources are spread throughout the organization, not all technology is under the control of the IT department, a higher level position may be more appropriate for Y2K responsibility.

7. Are senior management aware of the Year 2000 issue?

Yes	**209**	No	**17**	Blank	**56**
	74%		**6%**		**20%**

Auditor's Comment: Because it is critical that support for corrective action on the Y2K issue be forthcoming from the highest levels within each organization, we are concerned that 26% of the entities responding indicated that management was unaware, or did not know whether management was aware of the year 2000 problem. This would imply that approximately one out of every four senior management teams was unaware of the Y2K problem.

8. Has a Year 2000 Project been established?

Yes	**91**	No	**130**	Blank	**61**
	32%		**46%**		**22%**

Auditor's Comment: Regarding the establishment of a Y2K project, the survey indicated that approximately 1/3 of those entities responding had established a Y2K project. It is likely that there was a high number of entities that had not established a Y2K project because they had not yet performed a Y2K analysis and, therefore, were unsure of the nature and extent of their Y2K project.

9. Has a formal timetable been established for Year 2000 Project?

Yes	**54**	No	**167**	Blank	**61**
	19%		**59%**		**22%**

Auditor's Comment: The figures above indicate that there was a portion of the established Y2K projects that did not have timetables. It is possible that the relatively low number of entities indicating that a Y2K timetable had been established was a result of the same cause provided in question number 8 above.

10. Are user management actively involved in the project's progress?

Yes	**82**	No	**130**	Blank	**70**
	29%		**46%**		**25%**

Auditor's Comment: The survey indicated that only 29% of user management was actively involved in the Y2K project's progress. Considering that 58% of the entities responding had initiated efforts to ensure that their systems were Y2K compliant (see question number 3 under Awareness), it is of concern that there is, apparently, a large segment of entities not involving user management in the process. We believe that greater user management involvement during identification and assessment of systems and technology would assist in establishing or confirming priorities for remedial action. It is also important to ensure that there is adequate user involvement during the testing phase to determine whether modified systems are operating as intended and to validate remedial action.

II. Assessment

1. Has your organization started a Year 2000 assessment?

Yes	**111**	No	**91**	Blank	**80**
	39%		**32%**		**29%**

Date initiated (month / year): **90 responses, ranging from June 1990 to November 1997.**

Auditor's Comment: The survey figures indicate a significant delay in initiating Y2K assessments, with approximately 61% of the responding entities stating that they had not begun an assessment or had left the question blank. Given that 81% of the entities responding had indicated that they were aware of the Y2K problem, it appears that, for many entities, awareness of the problem had yet to be translated into action.

2. Has your organization completed a Year 2000 assessment?

Yes		No		Blank	
	45		**170**		**67**
	16%		**60%**		**24%**

Date initiated (month / year): 66 responses, ranging from October 1985 to December 1997.

Auditor's Comment: The figures indicate that less that one fifth of the entities responding had completed their Y2K assessments. Although interviews conducted during and after the survey indicate that additional assessments have been completed, we believe that the Commonwealth as a whole is significantly behind regarding assessments of the entire information systems and technology environment.

3. When are you planning to complete the Year 2000 project, (e.g., changes made, tested, and moved into production)? **66 responses, ranging from 1985 to July 2000.**

Auditor's Comment: While acknowledging that delays in conducting assessments and developing Y2K strategies will inhibit efforts to establish project deadlines, the low level of response indicates that established project plans may not be in place or sufficiently complete to ensure that Y2K compliance is attained in time.

4. What steps have been taken to assess the impact of Year 2000 on applications? e.g., have inventories been made of:

114	applications / programs performing date calculations
106	packaged software (supported and unsupported)
54	end-user developed applications
30	programs where source code is not available
57	program languages (supported and unsupported)
81	databases where dates form part of a key field
49	interfaces to / from third parties
85	operating systems (supported and unsupported)
44	security systems
81	database systems
46	compilers (may or may not support Year 2000)
30	firmware
22	other system software

Auditor's Comment: The figures above indicate that assessment efforts have been focused on application systems and to a lesser degree on system software and firmware. We believe that this is illustrative of beginning assessment efforts with focus placed on traditional business application systems. It may also indicate that entities will either defer their focus on supporting technology, or believe that the hardware and software vendor community will address the infrastructure in time. Regarding this question, we are concerned that the technology infrastructure may not be adequately assessed in time and that corrective strategies may be adversely impacted. In addition, entities indicating that source code is unavailable may be presented with a major problem in cases where those software products are not going to attain Y2K compliance by the vendor.

5. Indicate types of platforms inventoried for Year 2000 assessment:

23	mainframes	**76**	minicomputers	**40**	Other _______
62	LANs	**65**	microcomputers	**12**	N A

Auditor's Comment: The figures above are troubling because they do not adequately reflect the total resources of the Commonwealth's IT environment. Clearly, it is important to identify the complete information technology environment. Given the pervasive nature of technology, accurate and complete identification of all platforms may lead to discovering important systems requiring Y2K remedial action.

6. Provide date when Year 2000 will first impact your information systems:

96 responses, ranging from April 1997 to January 2000.

7. Have critical event horizons been established for key business activities?

Yes	**50**	No	**124**	Blank	**108**
	18%		**44%**		**38%**

Auditor's Comment: The figures above indicate that very few entities were able to identify initial impact of Year 2000. Entities should be able to identify first impact dates as soon as they have completed their assessments.

8. What methodology did you use to develop your estimates of information technology costs?

14	Line of code estimate
25	FTE requirement estimate
21	Function point estimation
62	Other ______________________________

9. What is your current estimate of Year 2000 costs?

a)	Total Cost	**64 responses, ranging from $0 to $27,000,000, totaling $70,000,000**
b)	IT Costs	**32 responses, ranging from $0 to $7,600,000**
c)	Cost per line of code	**31 responses, ranging from $0.06 to $2.00**

10. Estimated cost to replace hardware because of Year 2000 incompatibility
47 responses, totaling $33,980,000

11. Estimated cost to modify software
41 responses, totaling $14,666,820

12. Estimated cost to replace software
66 responses, totaling $3,310,100

13. Date by which all coding changes are estimated to be completed:
90 responses, ranging from April 1997 to July 2000

14. What are your costs estimates by fiscal year? **147** Not determined
1997 **39** 1998 **46** 1999 **33** 2000 **17**

Auditor's Comment: For questions 8 through 14, the figures provided indicate that, as of the survey date ,few entities were able to estimate their total costs for Y2K projects. Given that most agencies were either at the beginning of their assessments, or had not taken any action at that time, a reliable total cost estimate for the Commonwealth is unavailable. Based on interviews conducted during and after the survey, there also appears to be some confusion about what costs will actually be attributable to Y2K. Given that only 5% of the entities surveyed provided cost figures, and that assessments and Y2K strategies were yet to be completed for the majority of state entities, anticipated total costs could be significantly higher.

15. What proportion of the year 2000 work will be done in-house, and how much will be out-sourced?
in-house **Range: 0 to 100%** out-sourced **Range: 0 to 100%**

% in-house:	**78**	% out-sourced	**57**	Not determined	**147**
	28%		**20%**		**52%**

Auditor's Comment: Because of the low level of responses, funding requirements for outsourcing cannot be drawn from the survey. Based on our interviews, it appears that most entities do not have the resources internally to address Y2K on their own.

16. Have vendors already been engaged for any phases of the Year 2000 project?

Yes	**60**	No	**143**	Blank	**79**
	21%		**51%**		**28%**

Auditor's Comment: With respect to outsourcing, we are concerned that resources may be unavailable when needed by entities which are late in determining their Y2K requirements.

17. Has an assessment been made of the staff needed to test the changes made for Year 2000?

Yes	**58**	No	**142**	Blank	**82**
	21%		**50%**		**29%**

Auditor's Comment: The above figures are reflective of the fact that most entities are in the earlier stages of addressing Y2K, or have not taken action. The longer entities wait to determine staffing requirements, the more difficult and costly it may become to acquire qualified staff because competitive forces in the marketplace and time are combining to work against obtaining additional competent staff.

18. What are your expected staffing (FTE) requirements to address Year 2000 for Calendar Years:

1997	**50 responses, ranging from 0 to 14.**
1998	**51 responses, ranging from 0 to 43.**
1999	**49 responses, ranging from 0 to 18.**
2000	**35 responses, ranging from 0 to 20.**

19. Has an assessment been made of any additional hardware capacity requirements?

Yes	**63**	No	**141**	Blank	**78**
	22%		**50%**		**28%**

Auditor's Comment: The figures imply that almost 25% of the entities responding had assessed the need for additional hardware capacity. The high number of entities that have not determined their hardware capacity requirements (78%) may be a direct result of delays in completing their assessments. Significant delays in assessing and acquiring needed hardware capacity could adversely impact Y2K testing and subsequent implementation of compliant systems.

20. Have you performed a risk assessment of the vulnerability of your programs and applications for the year 2000 problem?

Yes	**57**	No	**140**	Blank	**85**
	20%		**50%**		**30%**

Auditor's Comment: The above figures reflect a general lack of completeness of Y2K assessments. Failure to assess the vulnerabilities of information systems and technology for Y2K compliance could adversely impact decisions regarding remedial actions or the development of contingency plans.

21. If one is planned, indicate when it is expected to be completed:

40 responses, ranging from October 1985 to September 1999.

22. Does your organization transmit data to other organizations?

Yes	**144**	No	**64**	Blank	**74**
	51%		**23%**		**26%**

If yes, identify org(s): **131 responses** were provided. Included responses indicated that data is transmitted to other state agencies, the federal government, courts, banks, vendors, and municipalities.

23. Does your organization receive data from other organizations?

Yes	**136**	No	**70**	Blank	**76**
	48%		**25%**		**27%**

Auditor's Comment: The above figures indicate the growing interdependencies of technology between and among state entities and outside parties. Given the increased use of electronic commerce and electronic data interchange (EDI), it is important that entities electronically transmitting and receiving data ensure that their Y2K fixes and date formats are compatible with those of corresponding entities to help prevent the loss of data and system integrity.

If yes, identify org(s): **65 responses** were provided. Included responses indicated that data is received from other state agencies, the federal government, courts, banks, vendors, and municipalities.

24. Have you evaluated the vulnerability of your agency's systems and applications to external organizations that fail to modify their own systems for the year 2000 problem?

Yes	**42**	No	**157**	Blank	**83**
	15%		**56%**		**29%**

25. If yes, was the assessment done with input from the affected parties?

Yes	**17**	No	**52**	Blank	**213**
	6%		**18%**		**76%**

26. What is the size of your information technology application portfolio?

a)	Number of lines:	**44 responses, ranging from 0 to 13,830,792**
b)	Number of applications:	**85 responses, ranging 0 to 1,865**
c)	Number of interfaces:	**59 responses, ranging from 0 to 500**

27. Has the agency performed an assessment of the impact on:

39	Tape / archive management systems where dates such as 9/9/99 or 31/12/99 could have been used to indicate the data should not be deleted.
45	PBX and other communication systems that may be date dependent.
20	Electronic security and alarm systems that are date dependent.
	Other IT dependent systems, specify:

16 responses were provided. Included responses indicated that other IT dependent systems were: all major MIS applications, completing assessment, license database, RMV data center, and simulators.

Auditor's Comment: The figures indicate that only a small portion of state entities have evaluated risks associated with dependency or corruptibility of non-business application systems.

28. Does the agency software inventory identify, for each application, system the following:

78	system owners and or users
28	total lines of code
69	software language
53	interfaces
72	platform(s) supporting the applications

29. Has all software been evaluated for Year 2000 compliance?

Yes	**60**	No	**129**	Blank	**93**
	21%		**46%**		**33%**

a)	If Yes: software that is Year 2000 compliant	(est.)	**56 responses, range: 0 to 100 %**
b)	If Yes: software that is NOT Year 2000 compliant	(est.)	**39 responses, range: 2 to 100 %**

Auditor's Comment: The high number of entities indicating that not all software has been evaluated, together with those which did not provide a response, is indicative of the relative incompleteness of assessments at the time of the survey.

30. Number of lines of software needing modification because of Year 2000
34 responses, ranging from 80 to 5,700,000.

31. Does your agency depend on vendor software products that will need to become Year 2000 compliant?

Yes	**145**	No	**50**	Blank	**87**
	51%		**18%**		**31%**

32. Have you confirmed package software compliance?

Yes	**85**	No	**103**	Blank	**94**
	30%		**37%**		**33%**

33.	Total number of software packages to be modified	**92 responses, range 0 to 716**
34.	Number software packages to be modified by third party vendor	**86 responses, range: 0 to 710**
35.	Number software packages to be modified by internal staff	**78 responses, range: 0 to 7**

36. Have data files, both internal and those shared with others been reviewed?

Yes	**71**	No	**112**	Blank	**99**
	25%		**40%**		**35%**

37. Will you require additional capacity for DASD, testing, CPU, for conversion?

Yes	**41**	No	**96**	Blank	**145**
	15%		**34%**		**51%**

Auditor's Comment: The large number of blank responses might be expected given that a significant portion of entities have not completed their hardware capacity analysis. (See question 19 in this section.)

38. Will you need assistance in identifying additional resources, (i.e., vendors, tools)?

Yes	**77**	No	**98**	Blank	**107**
	27%		**35%**		**38%**

39. Are programs missing source code?

Yes	**20**	No	**84**	Don't Know	**86**	Blank	**92**
	7%		**30%**		**30%**		**33%**

40. Is system documentation accurate and up to date?

Yes	**86**	No	**42**	Don't Know	**61**	Blank	**93**
	30%		**15%**		**22%**		**33%**

41. Are there problems currently being experienced in regard to year 2000?

Yes	**16**	No	**141**	Don't Know	**42**	Blank	**83**
	6%		**50%**	**15%**		**29%**	

III. Planning

1. Does your organization have a written and approved Year 2000 plan?

Yes	**14**	No	**190**	Blank	**78**
	5%		**67%**		**28%**

a) If No, will you need assistance in developing a Year 2000 plan?

Yes	**77**	No	**98**	Blank	**107**
	27%		**35%**		**38%**

b) If Yes, has the Year 2000 plan been approved by your SIO or CIO?

Yes	**14**	No	**50**	Blank	**218**
	5%		**18%**		**77%**

2. What actions relating to Year 2000 have been approved by management:

84 responses were provided. Included responses indicated: buy new equipment, modify priority systems, assessment and scope, temporary patch on minicomputers, all actions, all plans, confirm vendor plans, assess own data, database upgrade, inventory and assessment, none deemed necessary, planning and research, replace all COBOL systems, software upgrade, and under advisement.

3. What priorities have been established:

61 responses were provided. Included responses indicated priorities of administrative systems and phone systems, complete by July 1998, licensing and examination programs, mission-critical applications, and pending.

4. What timetable has been set: **60 responses, ranging from 1997 to 1999**

5. % IT to replace **26 responses, ranging from 0 to 100%**

6. % IT to repair **24 responses, ranging from 0 to 100%**

7. % IT not impacted **28 responses, ranging from 0 to 100%**

8. Strategies being considered for resolving Year 2000 problems:

94	change all dates to four-digit years
20	develop program solutions and keep two-digit years
18	big-bang or piecemeal developments
18	bridge programs
86	rely on package vendors to supply solutions

9. Have you developed a prioritization of which systems need to be fixed in order to avoid an adverse impact òn the public?

Yes	**88**	No	77	Blank	**117**
	31%		**27%**		**42%**

10. Does your Year 2000 plan contain specific timetables and milestones?

Yes	**40**	No	**76**	Blank	**166**
	14%		**27%**		**59%**

11. How is application code being made year 2000 compliant? (Please select one.)

45	Year 2000 changes mostly performed during normal production modifications
9	Application code is "frozen" while year 2000 changes are made
30	Application code has both year 2000 changes and production modification occurring simultaneously.

12. Are vendor-supplied products being used to make year 2000 changes?

Yes	**33**	No	**120**

If yes, please list tools used: **23 responses,** indicating various vendor products.

13. Have you selected tool sets and methodologies?

Yes	**27**	No	**135**	Blank	**120**
	10%		**48%**		**42%**

14. Phases of your Year 2000 effort for which vendors are being used: (Please select all that apply.)

26	Planning	**21**	Repair
15	Inventory	**9**	Code Merge
29	Assessment	**20**	Testing
16	Other:______________________________		

15. Steps taken to mitigate risk: (Please select all that apply.)

58	None
4	Business units have created contingency plans
7	Risks have been scored and target mitigation levels set for the life of the Year 2000 initiative
49	Prioritizing systems to ensure high value systems are supported
2	Planning to shut down low priority business operations
29	Don't know
26	Other: ____

16. Do you have documented contingency plans for your year 2000 project if your agency is unable to complete your year 2000 plan as scheduled?

Yes	**5**	No	**164**	Blank	**113**
	2%		**58%**		**40%**

17. Are you using the CCYY-MM-DD standard as adopted by NIST, ISO and the Commonwealth of Massachusetts for EDI among its agencies?

Yes	**85**	No	**59**	Blank	**138**
	30%		**21%**		**49%**

18. If not, what other Year 2000 standards have been established for on-going enhancements and future developments?

36 responses were provided. Included responses indicated standards of: dd/yyyy, Julian date format, mm/dd/ccyy, perpetual calendar; that respondents rely on vendors, or answer unknown.

19. Have you assigned owners and sponsors to the project tasks?

Yes	**56**	No	**121**	Blank	**105**
	20%		**43%**		**37%**

20. Have you contacted current or future vendors regarding compliance?

Yes	**89**	No	**93**	Blank	**100**
	32%		**33%**		**35%**

21. Have you appointed a year 2000 coordinator?

Yes	**100**	No	**82**	Blank	**100**
	35%		**30%**		**35%**

22. Have you selected support resources?

Yes	**44**	No	**134**	Blank	**104**
	16%		**47%**		**37%**

23. Have you assembled a project team?

Yes	**66**	No	**112**	Blank	**104**
	23%		**40%**		**37%**

24. Have you converted or replaced systems?

Yes	**47**	No	**132**	Blank	**103**
	17%		**47%**		**36%**

Auditor's Comment: The above figures support the conclusion that there is a minority of state entities that have taken steps to address Y2K. To improve that number, entities need to quickly complete their assessments, project plans, remedial programming activities, and required testing.

IV. System Modification

1. What conversion work or piloting of conversions has been carried out?

   111 responses were provided. Included responses indicated: some batch, assessment of on-line process, database conversion, expanded year fields, none to date/must await changes currently applied to MMARS/warehouse sources, presently under advisement, several projects started, total system re-design, and working on pilot section.

2. Has all software been made Year 2000 compliant?

Yes	**21**	No	**143**	Blank	**118**
	7%		**51%**		**42%**

Auditor's Comment: Based on interviews with ITD, we would expect that this number would increase.

3. Is your agency meeting its budget and schedule in the conversion of targeted applications, platforms, databases, archives, and interfaces?

Yes	**68**	No	**46**	Blank	**168**
	24%		**16%**		**60%**

4. Is your agency meeting its budget and scheduling in the development of bridges and filters to handle non-compliant data?

Yes	**41**	No	**42**	Blank	**199**
	15%		**15%**		**70%**

5. Is your agency meeting its budget and schedule in the replacement of targeted applications and system components?

Yes	**56**	No	**39**	Blank	**187**
	20%		**14%**		**66%**

6. Is your agency documenting all code and system modifications and using program change management techniques and/or software?

Yes	**57**	No	**54**	Blank	**171**
	20%		**19%**		**61%**

7. Is your agency scheduling unit, system, and integration tests for all modified software?

Yes	**57**	No	**53**	Blank	**172**
	20%		**19%**		**61%**

8. Is your agency meeting its budget and schedule in eliminating targeted applications and system components?

Yes	**55**	No	**38**	Blank	**189**
	20%		**14%**		**66%**

9. Is your agency communicating all changes to its information systems to all internal and external users?

Yes	**63**	No	**53**	Blank	**166**
	22%		**19%**		**59%**

10. Is your agency tracking the conversion and replacement process and collecting and using project-related statistics to manage the conversion and replacement process?

Yes	**40**	No	**74**	Blank	**168**
	14%		**26%**		**60%**

11. Is your agency sharing information among Year 2000 projects?

Yes	**52**	No	**72**	Blank	**158**
	19%		**26%**		**55%**

V. Testing

1. Has your agency developed and documented test and validation plans for each converted or replaced application or system component?

Yes	**22**	No	**136**	Blank	**124**
	8%		**48%**		**44%**

2. Has your agency developed and documented a strategy for testing contractor converted or replaced applications or system components?

Yes	**31**	No	**115**	Blank	**136**
	11%		**41%**		**48%**

3. Has your agency implemented a year 2000 test facility?

Yes	**16**	No	**141**	Blank	**125**
	6%		**50%**		**44%**

4. Has your agency implemented automated test tools and scripts?

Yes	**7**	No	**146**	Blank	**129**
	2%		**52%**		**46%**

5. Has your agency performed unit, system, and integration tests on each converted or replaced component?

Yes	**20**	No	**130**	Blank	**132**
	7%		**46%**		**47%**

6. Your agency's testing procedures include the following types of tests:

14	regression
44	performance
16	stress
29	forward and backward

7. Is your agency tracking the testing and validation process and collecting and using project-related statistics to manage the process?

Yes	**22**	No	**119**	Blank	**141**
	8%		**42%**		**50%**

8. Has your agency initiated acceptance testing?

Yes	**18**	No	**121**	Blank	**143**
	6%		**43%**		**51%**

VI. Implement New Software

1. Has your agency defined its transition environment and procedures?

Yes	**53**	No	**112**	Blank	**117**
	19%		**40%**		**41%**

2. Has your agency developed and documented a schedule for the implementation of all converted or replaced applications and system components?

Yes	**43**	No	**117**	Blank	**122**
	15%		**42%**		**43%**

3. Has your agency resolved all data exchange issues and interagency concerns?

Yes	**22**	No	**133**	Blank	**127**
	8%		**47%**		**45%**

4. Has your agency dealt with database and archive conversions?

Yes	**41**	No	**113**	Blank	**128**
	15%		**40%**		**45%**

5. Has your agency completed acceptance testing?

Yes	**8**	No	**146**	Blank	**128**
	3%		**52%**		**45%**

6. Has your agency developed contingency plans?

Yes	**7**	No	**140**	Blank	**135**
	2%		**50%**		**48%**

7. Has your agency updated or developed disaster recovery and business continuity plans?

Yes	**24**	No	**133**	Blank	**125**
	9%		**47%**		**44%**

8. Has your agency reintegrated the converted and replaced systems and related data?

Yes	**14**	No	**135**	Blank	**123**
	5%		**50%**		**45%**

VII. Other

1. What barriers have you encountered in carrying out your Year 2000 project, (e.g., lack of resources, uncooperative partners) and how have you addressed them?

Barrier: **87 responses. The following is a partial list of recurring problems identified**:

- Lack of official structure to deal with Year 2000
- Lack of management attention, direction, and planning
- Lack of capable personnel
- Lack of funding
- Lack of other resources
- Lack of knowledge and information regarding the topic
- Lack of communications
- Competing priorities

Solution: ____________**No responses**____

2. When was the last time your agency produced a status report on the year 2000 project?

54 responses were provided. Included responses indicated: weekly or biweekly, periodic, or none. Dates between March and June 1997 were also provided.

3. Does your organization have access to the Internet?

Yes	**111**	No	**52**	Blank	**119**
	40%		**18%**		**42%**

4. How would you prefer to be communicated with regard to Year 2000 issues?

85	Email / Internet

93 Hard copy mailings

43 Attending work group meetings

29 Phone call with contact person

5 Other____________________________

Appendix 2
Survey Population and Respondents

The following is a listing of entities to which year 2000 survey questionnaires were distributed through our mailing or through ITD's Year 2000 Meeting the Challenge publication. The list indicates the date that our office received a response to the survey. We acknowledge that for some entities for which no response date is provided, the entity may have considered that they were included in the response of a parent entity. In some instances, an administrative office or division may have responded for a department reporting to them.

Agencies

Administering Agency for Developmental Disabilities	4/30/97
Alcoholic Beverage Control Commission	9/3/97
Bay Cove Mental Health Center	8/19/97
Bridgewater Treatment Center	
Brockton Multi-Service Center	5/19/97
Bureau of Special Investigations	5/19/97
Bureau of State Buildings	6/10/97
Cambridge-Somerville Mental Health Center	9/8/97
Chelsea Soldiers' Home	4/28/97
Civil Service Commission	6/20/97
Committee on Criminal Justice	5/19/97
Cooperation for Business and Learning	
Department of Corrections	4/30/97
Department of Economic Development	5/19/97
Department of Education	6/24/97
Department of Environmental Management	5/30/97
Department of Environmental Protection	5/19/97
Department of Fisheries, Wildlife and Environmental Law Enforcement	8/22/97
Department of Food and Agriculture	
Department of Housing and Community Development	5/19/97
Department of Industrial Accidents	6/10/97
Department of Labor And Work Force Development	7/16/97
Department of Marine Fisheries	8/22/97
Department of Mental Health	5/19/97
Department of Mental Retardation	6/24/97
Department of Public Health	9/22/97
Department of Public Safety	5/19/97
Department of Public Utilities	5/19/97
Department of Revenue	5/19/97
Department of Social Services	6/24/97
Department of Transitional Assistance	6/19/97
Department of Veterans' Services	5/19/97
Disability Determination Services	
Division of Banks	6/18/97
Division of Capital Planning and Operations	9/9/97
Division of Conservation Services	4/28/97
Division of Employment And Training	5/19/97
Division of Energy Resources	5/15/97
Division of Health Care Finance and Policy	5/19/97
Division of Insurance	5/19/97
Division of Registration	9/23/97
Division of Standards	9/24/97
Division of Water Resources	
Division of Waterways	
DMR Fernald Center	9/8/97
DMR Hogan Regional Center	9/8/97
DMR Irving A. Glavin Regional Center	9/8/97
Dr. John C. Corrigan Mental Health Center	9/8/97
Dr. Solomon Carter Fuller Mental Health Center	9/8/97
Environmental Law Enforcement	8/22/97
Erich Lindemann Mental Health Center	8/19/97
Executive Office for Administration and Finance	6/20/97
Executive Office of Elder Affairs	9/29/97
Executive Office of Environmental Affairs	5/30/97
Executive Office of Health and Human Services	5/19/97
Executive Office of Public Safety	5/30/97
Executive Office of Transportation and Construction	10/7/97
Fall River Line Pier	
Fire Fighting Academy	
Fiscal Affairs Division	5/19/97
Forest and Parks Division	
George Fingold Library	
Group Insurance Commission	7/24/97
Hampden County Detention Center	5/20/97
Hazardous Waste Site Safety Council	
Higher Education Coordinating Council	5/14/97
Holyoke Soldiers' Home	5/1/97
Human Resources Division	6/20/97
Information Technology Division	5/19/97
Joint Labor Management Committee	5/13/97
Law Enforcement	
Marine Fisheries Annisquam River	8/22/97
Massachusetts Arts Lottery Council	
Massachusetts Convention Center	
Massachusetts Criminal Justice Training Council	5/30/97
Massachusetts Cultural Council	5/19/97
Massachusetts District Attorneys' Association	8/6/97
Massachusetts Board of Higher Education	5/15/97

Massachusetts Emergency Management Agency	5/19/97
Massachusetts Highway Department	5/19/97
Massachusetts Housing Finance Agency	5/19/97
Massachusetts Mental Health Center	
Massachusetts National Guard	
Massachusetts Office on Disability	5/2/97
MCI Massachusetts Boot Camp	6/26/97
MCI Bay State Correctional Center	6/26/97
MCI Boston Pre-Release Center	6/26/97
MCI Bridgewater State Hospital	6/26/97
MCI Cedar Junction	6/26/97
MCI Concord	6/26/97
MCI Framingham	6/26/97
MCI Lancaster	6/26/97
MCI Longwood Treatment Center	6/26/97
MCI Norfolk	6/26/97
MCI Northeast Correction Center	6/26/97
MCI Old Colony Correction Center	6/26/97
MCI Park Drive Pre-Release	6/26/97
MCI Plymouth	6/26/97
MCI Pondville Correction Center	6/26/97
MCI South Middlesex Correctional Center	6/26/97
MCI Southeastern Correctional Center	6/26/97
MCI-Shirley, Shirley Pre-Release Center	6/26/97
Mental Health Legal Advisors Committee	8/19/97

Metro Area Planning Council	
Monson Developmental Center	
New Chardon Street Home for Women	
North Central Correctional Institute	6/26/97
Northern Middlesex Council of Governments	9/8/97
Office for Children	8/26/97
Office of Campaign and Political Finance	9/16/97
Office of Consumer Affairs and Business Regulations	9/24/97
Office of the Chief Medical Examiner	
Office of the Inspector General	8/25/97
Office of the State Comptroller	4/17/97
Old Colony Planning Council	
Operational Services Division	6/19/97
Paul A. Dever State School	9/8/97
Quincy Mental Health Center	8/19/97
Registry of Motor Vehicles	5/19/97
Sergeant At Arms	
Solid Waste Management	
State Board of Retirement	
Water Pollution Control	5/19/97
Western Massachusetts Area Office	5/14/97
Wrentham State School	9/8/97
Youth Services	6/2/97

Authorities – Housing

Abington Housing Authority	
Acton Housing Authority	5/19/97
Acushnet Housing Authority	
Adams Housing Authority	6/18/97
Agawam Housing Authority	6/10/97
Amesbury Housing Authority	6/18/97
Amherst Housing Authority	5/9/97
Andover Housing Authority	5/19/97
Arlington Housing Authority	6/19/97
Ashland Housing Authority	
Athol Housing Authority	
Attleboro Housing Authority	
Auburn Housing Authority	5/19/97
Avon Housing Authority	6/18/97
Ayer Housing Authority	6/19/97
Barnstable Housing Authority	5/14/97
Barre Housing Authority	6/4/97
Bedford Housing Authority	5/5/97
Belchertown Housing Authority	
Bellingham Housing Authority	6/19/97
Belmont Housing Authority	7/9/97
Berkshire County Regional Housing Authority	
Beverly Housing Authority	6/18/97
Billerica Housing Authority	8/11/97
Blackstone Housing Authority	4/29/97
Boston Housing Authority	

Bourne Housing Authority	
Braintree Housing Authority	5/19/97
Brewster Housing Authority	5/1/97
Bridgewater Housing Authority	7/25/97
Brimfield Housing Authority	
Brockton Housing Authority	
Brookfield Housing Authority	
Brookline Housing Authority	
Burlington Housing Authority	7/9/97
Cambridge Housing Authority	7/1/97
Canton Housing Authority	5/15/97
Carver Housing Authority	5/2/97
Charlton Housing Authority	
Chatham Housing Authority	5/6/97
Chelmsford Housing Authority	
Chelsea Housing Authority	6/20/97
Chicopee Housing Authority	
Clinton Housing Authority	5/13/97
Cohasset Housing Authority	
Concord Housing Authority	
Dalton Housing Authority	6/19/97
Danvers Housing Authority	4/30/97
Dartmouth Housing Authority	5/2/97
Dedham Housing Authority	7/24/97
Dennis Housing Authority	5/1/97
Dighton Housing Authority	5/13/97

Douglas Housing Authority	
Dracut Housing Authority	
Dudley Housing Authority	5/8/97
Dukes County Regional Housing Authority	6/18/97
Duxbury Housing Authority	
East Bridgewater Housing Authority	
East Longmeadow Housing Authority	
Easthampton Housing Authority	
Easton Housing Authority	
Essex Housing Authority	
Everett Housing Authority	
Fairhaven Housing Authority	6/4/97
Fall River Housing Authority	
Falmouth Housing Authority	
Fitchburg Housing Authority	
Foxboro Housing Authority	6/19/97
Framingham Housing Authority	
Franklin County Regional Housing Authority	6/19/97
Franklin Housing Authority	
Gardner Housing Authority	5/20/97
Georgetown Housing Authority	
Gloucester Housing Authority	
Grafton Housing Authority	
Granby Housing Authority	
Great Barrington Housing Authority	5/7/97
Greenfield Housing Authority	6/19/97
Groton Housing Authority	
Groveland Housing Authority	
Hadley Housing Authority	5/19/97
Halifax Housing Authority	
Hamilton Housing Authority	6/18/97
Hampden Housing Authority	
Hampshire County Regional Housing Authority	5/19/97
Hanover Housing Authority	
Hanson Housing Authority	5/7/97
Harwich Housing Authority	
Hatfield Housing Authority	
Haverhill Housing Authority	
Hingham Housing Authority	
Holbrook Housing Authority	
Holden Housing Authority	6/18/97
Holliston Housing Authority	
Holyoke Housing Authority	
Hopedale Housing Authority	6/18/97
Hopkinton Housing Authority	
Hudson Housing Authority	
Hull Housing Authority	
Ipswich Housing Authority	5/7/97
Kingston Housing Authority	

Lancaster Housing Authority	
Lawrence Housing Authority	
Lee Housing Authority	
Leicester Housing Authority	
Lenox Housing Authority	6/18/97
Leominster Housing Authority	7/9/97
Lexington Housing Authority	
Littleton Housing Authority	
Longmeadow Housing Authority	5/6/97
Lowell Housing Authority	7/31/97
Ludlow Housing Authority	5/8/97
Lunenburg Housing Authority	
Lynn Housing Authority	
Lynnfield Housing Authority	5/6/97
Malden Housing Authority	
Manchester Housing Authority	
Mansfield Housing Authority	6/10/97
Marblehead Housing Authority	
Marlboro Housing Authority	
Marshfield Housing Authority	5/13/97
Mashpee Housing Authority	
Mattapoisett Housing Authority	9/22/97
Maynard Housing Authority	
Medfield Housing Authority	
Medford Housing Authority	
Medway Housing Authority	
Melrose Housing Authority	
Mendon Housing Authority	
Merrimac Housing Authority	
Methuen Housing Authority	
Middleboro Housing Authority	
Middleton Housing Authority	
Millbury Housing Authority	
Millis Housing Authority	
Milton Housing Authority	5/8/97
Milford Housing Authority	5/19/97
Monson Housing Authority	
Montague Housing Authority	
Nahant Housing Authority	5/8/97
Nantucket Housing Authority	5/30/97
Natick Housing Authority	
Needham Housing Authority	
New Bedford Housing Authority	6/20/97
Newburyport Housing Authority	
Newton Housing Authority	5/1/97
Norfolk Housing Authority	
North Adams Housing Authority	5/2/97
North Andover Housing Authority	5/13/97
North Attleboro Housing Authority	
North Brookfield Housing Authority	
North Reading Housing Authority	
Northampton Housing Authority	

Northborough Housing Authority	5/1/97
Northbridge Housing Authority	
Norton Housing Authority	
Norwell Housing Authority	
Norwood Housing Authority	
Orange Housing Authority	5/5/97
Orleans Housing Authority	
Oxford Housing Authority	5/5/97
Palmer Housing Authority	
Peabody Housing Authority	5/13/97
Pembroke Housing Authority	
Pepperell Housing Authority	
Pittsfield Housing Authority	
Plainville Housing Authority	
Plymouth Housing Authority	
Provincetown Housing Authority	6/4/97
Quincy Housing Authority	5/19/97
Randolph Housing Authority	5/30/97
Raynham Housing Authority	5/19/97
Reading Housing Authority	
Rehoboth Housing Authority	
Revere Housing Authority	
Rockland Housing Authority	
Rockport Housing Authority	
Rowley Housing Authority	6/18/97
Salem Housing Authority	
Salisbury Housing Authority	5/7/97
Sandwich Housing Authority	6/24/97
Saugus Housing Authority	6/18/97
Scituate Housing Authority	6/18/97
Seekonk Housing Authority	6/20/97
Sharon Housing Authority	5/19/97
Shrewsbury Housing Authority	
Somerset Housing Authority	5/2/97
Somerville Housing Authority	6/24/97
South Hadley Housing Authority	5/1/97
Southampton Housing Authority	
Southborough Housing Authority	
Southbridge Housing Authority	
Southwick Housing Authority	4/30/97
Spencer Housing Authority	
Springfield Housing Authority	5/19/97
Sterling Housing Authority	5/22/97
Stockbridge Housing Authority	4/29/97
Stoneham Housing Authority	5/6/97
Stoughton Housing Authority	

Sturbridge Housing Authority	
Sudbury Housing Authority	5/6/97
Sutton Housing Authority	5/2/97
Swampscott Housing Authority	
Swansea Housing Authority	
Taunton Housing Authority	
Templeton Housing Authority	5/13/97
Tewksbury Housing Authority	
Topsfield Housing Authority	
Tyngsboro Housing Authority	
Upton Housing Authority	
Uxbridge Housing Authority	4/29/97
Wakefield Housing Authority	5/19/97
Walpole Housing Authority	9/16/97
Waltham Housing Authority	
Ware Housing Authority	
Wareham Housing Authority	
Warren Housing Authority	5/14/97
Watertown Housing Authority	
Wayland Housing Authority	
Webster Housing Authority	
Wellesley Housing Authority	6/30/97
Wenham Housing Authority	
West Boylston Housing Authority	
West Bridgewater Housing Authority	
West Brookfield Housing Authority	6/4/97
West Newbury Housing Authority	5/22/97
West Springfield Housing Authority	5/22/97
Westborough Housing Authority	5/1/97
Westfield Housing Authority	5/14/97
Westford Housing Authority	5/1/97
Westminster Housing Authority	5/14/97
Westport Housing Authority	
Weymouth Housing Authority	
Whitman Housing Authority	
Wilbraham Housing Authority	
Williamstown Housing Authority	5/13/97
Wilmington Housing Authority	
Winchendon Housing Authority	4/30/97
Winchester Housing Authority	
Winthrop Housing Authority	
Woburn Housing Authority	8/26/97
Worcester Housing Authority	
Wrentham Housing Authority	
Yarmouth Housing Authority	

Authorities – Other

Bourne Recreation Authority	
Massachusetts Bay Transportation Authority	5/15/97
Massachusetts Development Authority	6/18/97
Massachusetts Port Authority	6/10/97
Massachusetts State College Building Authority	

Massachusetts Turnpike Authority	5/20/97
Massachusetts Water Resources Authority	5/19/97
Southeastern Mass University. Building Authority	5/2/97
Steamship Authority	9/29/97

Boards and Commissions

Appellate Tax Board	5/19/97
Architectural Access Board	5/19/97
Art Commission	4/24/97
Ballot Law Commission	
Berkshire Regional Planning Commission	
Board of Library Commissioners	
Board of Registration of Medicine	
Boxers Fund Board	
Cape Cod Planning Economic Commission	
Central Massachusetts Planning Commission	
Commission Against Discrimination	6/20/97
Commission for the Blind	5/19/97
Commission for The Deaf and Hard of Hearing	5/19/97
Commission on Judicial Conduct	6/18/97
Criminal History Systems Board	6/18/97
Disabled Persons Protection Commission	
Energy Facilities Siting Board	
Franklin County Planning Commission	
Labor Relations Commission	6/18/97
Lottery Commission	7/22/97
Massachusetts Aeronautics Commission	5/19/97

Massachusetts Cable Television Commission	7/2/97
Massachusetts Historical Commission	8/25/97
Massachusetts Rehabilitation Commission	6/2/97
Merit Rating Board	5/19/97
Merrimac Valley Planning Commission	5/20/97
Metropolitan District Commission	
Montachusett Region Planning Commission	
New England Board of Education	
Outdoor Advertising Board	5/20/97
Parole Board	8/5/97
Pioneer Valley Planning Commission	9/2/97
Public Access Board	8/26/97
Public Employee Retirement Admin. Commission	6/4/97
Records Conservation Board	9/8/97
Southeast Region Planning and Economic Commission	
State Ethics Commission	4/14/97
State Racing Commission	8/27/97
Teachers' Retirement Board	9/18/97
Victim Witness Assistance Board	9/2/97

Colleges and Universities

Berkshire Community College	9/16/97
Bridgewater State College	6/4/97
Bristol Community College	5/19/97
Bunker Hill Community College	5/6/97
Cape Cod Community College	9/16/97
Fitchburg State College	5/30/97
Framingham State College	5/19/97
Greenfield Community College	5/19/97
Holyoke Community College	5/19/97
Massachusetts Bay Community College	8/25/97
Massachusetts College of Art	5/19/97
Massachusetts Maritime Academy	5/19/97
Massasoit Community College	10/1/97
Middlesex Community College	5/19/97
Mount Wachusett Community College	5/19/97
North Adams State College	7/1/97

North Shore Community College	9/17/97
Northern Essex Community College	5/22/97
Quinsigamond Community College	8/25/97
Roxbury Community College	
Salem State College	
Springfield Technical Community College	5/15/97
University of Massachusetts	9/23/97
University of Massachusetts - Amherst	7/22/97
University of Massachusetts - Boston	7/22/97
University of Massachusetts Central Administrative Services	7/22/97
University of Massachusetts - Dartmouth	7/22/97
University of Massachusetts -Lowell	7/22/97
University of Massachusetts Medical Center	9/17/97
Westfield State College	5/7/97
Worcester State College	6/18/97

Constitutional Officers

Office of the State Auditor	9/23/97
Office of the Attorney General	9/16/97

Office of the Secretary of State	8/25/97
Office of the State Treasurer	9/18/97

District Attorneys

Barnstable District Attorney	8/15/97
Berkshire District Attorney	8/15/97
Bristol District Attorney	8/15/97
Cape and Islands District Attorney	8/15/97
Essex County District Attorney	8/15/97
Franklin Hampshire County District Attorney	9/23/97

Hampden District Attorney	8/15/97
Middlesex District Attorney	8/15/97
Norfolk County District Attorney	9/23/97
Plymouth District Attorney	8/15/97
Suffolk County District Attorney	8/15/97
Worcester County District Attorney	8/15/97

Governor

Governor's Council	5/5/97
Governor's Highway Safety Bureau	5/30/97

Governor's Office	6/20/97
Lieutenant Governor's Office	9/11/97

Hospitals

Lemuel Shattuck Hospital	6/10/97
Massachusetts Hospital School	6/18/97
Medfield State Hospital	8/26/97
Taunton State Hospital	8/20/97

Tewksbury Hospital	9/22/97
Westborough State Hospital	8/20/97
Western Massachusetts Hospital	8/14/97
Worcester State Hospital	8/20/97

Judiciary

Administrative Law Appeals	6/20/97
Administrative Office of Housing Court	
Administrative Office of Juvenile Courts	8/19/97
Administrative Office Probate and Family Court	8/19/97
Administrative Office District Courts	5/16/97
Administrative Office of the Superior Court	
Administrative Office of the Trial Court	7/1/97
Appeals Court	9/23/97
Attleboro District Court	8/19/97
Ayer District Court	5/16/97
Barnstable County Probate and Family Court	8/19/97
Barnstable District Court	8/19/97
Barnstable Superior Court	9/23/97
Berkshire County Probate and Family Court	8/19/97
Berkshire Superior Court	9/23/97
Boston Housing Court	8/19/97
Boston Juvenile Court	8/19/97
Boston Municipal Court	5/19/97
Brighton District Court	8/19/97
Bristol County Juvenile Court	8/19/97
Bristol County Probate and Family Court	5/7/97
Brockton District Court	8/19/97
Brookline District Court	8/19/97
Cambridge District Court	6/18/97
Charlestown District Court	8/19/97
Chelsea District Court	8/19/97
Chicopee District Court	8/19/97
Clinton District Court	8/19/97
Concord District Court	8/19/97
Court Facilities Bureau	9/23/97

Dedham District Court	8/19/97
Dorchester District Court	8/19/97
Dudley District Court	8/19/97
Dukes County Probate and Family Court	8/19/97
Dukes County Superior Court	5/6/97
East Boston District Court	8/19/97
East Brookfield District Court	8/19/97
Edgartown District Court	5/19/97
Essex County Probate and Family Court	5/5/97
Essex County Superior Court	9/23/97
Fall River District Court	5/19/97
Fitchburg District Court	8/19/97
Framingham District Court	5/30/97
Franklin County Probate and Family Court	5/2/97
Franklin Superior Court	9/23/97
Gardner District Court	8/19/97
Gloucester District Court	8/19/97
Greenfield District Court	5/19/97
Hampden County Housing Court	5/30/97
Hampden County Probate and Family Court	8/19/97
Hampden Superior Court	9/23/97
Hampshire County Probate and Family Court	6/20/97
Hampshire County Superior Court	5/19/97
Haverhill District Court	8/19/97
Hingham District Court	5/30/97
Holyoke District Court	5/19/97
Ipswich District Court	7/22/97
Land Court	7/7/97
Lawrence District Court	8/19/97
Leominster District Court	8/19/97

Lowell District Court	5/19/97
Lynn District Court	8/19/97
Malden District Court	8/19/97
Marlborough District Court	8/27/97
Middlesex County Probate and Family Court	8/19/97
Middlesex Juvenile Court	8/19/97
Middlesex Superior Court	8/19/97
Milford District Court	8/19/97
Nantucket District Court	8/19/97
Nantucket Probate and Family Court	8/19/97
Nantucket Superior Court	9/23/97
Natick District Court	8/19/97
New Bedford District Court	5/14/97
Newburyport District Court	8/19/97
Newton District Court	8/19/97
Norfolk County Probate and Family Court	8/19/97
Norfolk County Superior Court	9/23/97
North Essex Juvenile Probate Court	8/19/97
Northampton District Court	8/19/97
Northern Berkshire District Court	8/19/97
Office of the Commissioner of Probation	5/5/97
Office of the Jury Commissioner	5/7/97
Orange District Court	8/19/97
Orleans District Court	8/19/97
Palmer District Court	5/14/97
Peabody District Court	8/19/97
Pittsfield District Court	8/19/97
Plymouth County Juvenile Probate Court	8/19/97
Plymouth District Court	6/30/97
Plymouth Probate and Family Court	5/19/97

Plymouth Superior Court	9/23/97
Quincy District Court	8/19/97
Roxbury District Court	7/10/97
Salem District Court	5/13/97
Somerville District Court	5/7/97
South Boston District Court	8/19/97
Southern Berkshire District Court	8/19/97
Springfield District Court	8/19/97
Springfield Div Juvenile Court	8/19/97
Stoughton District Court	6/20/97
Suffolk County Probate and Family Court	8/19/97
Suffolk Superior Court	4/28/97
Superior Court House - New Bedford	9/23/97
Supreme Judicial Court	9/23/97
Taunton District Court	8/19/97
Uxbridge District Court	7/10/97
Waltham District Court	8/19/97
Ware District Court	6/4/97
Wareham District Court	8/19/97
West Roxbury Trial Court	7/7/97
Westborough District Court	7/7/97
Westfield District Court	8/19/97
Winchendon District Court	5/6/97
Woburn District Court	7/16/97
Worcester County Juvenile Court	8/19/97
Worcester County Probate and Family Court	8/19/97
Worcester District Court	8/19/97
Worcester Housing Court	8/19/97
Worcester Superior Court	9/23/97
Wrentham District Court	7/22/97

Legislative

House of Representatives	8/13/97
Legislative Post Audit Oversight Bureau	

Senate	9/30/97
Senate Post Audit Committee	7/1/97

Other

Children's Trust Fund	8/26/97
Community Economic Development Assistance Corporation	6/20/97
Government Land Bank	6/18/97
Greater Lawrence Sanitary District	5/13/97

Massachusetts Community Development Finance Corporation	
Massachusetts Technology Development Corporation	
Massachusetts Technology Park Corporation	

Regional Development Authorities

Arlington Regional Development Authority	
Attleboro Regional Development Authority	
Beverly Regional Development Authority	
Boston Regional Development Authority	
Cambridge Regional Development Authority	6/19/97
Fall River Regional Development Authority	

Fitchburg Regional Development Authority	
Gardner Regional Development Authority	4/30/97
Milford Regional Development Authority	
New Bedford Regional Development Authority	8/26/97
Newburyport Regional Development Authority	
Newton Community Development Authority	8/15/97

Northampton Regional Development Authority	
Plymouth Regional Development Authority	

Salem Regional Development Authority	

Regional Transit Authorities

Brockton Regional Transit Authority	5/30/97
Cape Ann Regional Transit Authority	5/13/97
Edgartown Regional Transit Authority	
Franklin County Regional Transit Authority	
Greenfield Montague Regional Transit Authority	
Lowell Regional Transit Authority	
Merrimac Valley Regional Transit Authority	5/19/97

Montachusett Regional Transit Authority	5/1/97
Pioneer Valley Regional Transit Authority	5/19/97
Stoughton Regional Development Authority	
Taunton Regional Development Authority	
Weymouth Regional Development Authority	
Woburn Regional Development Authority	
Worcester Regional Development Authority	

Appendix 3

List of Recommendations

The following is a list of the recommendations as they appear in the Survey Results section of the report. Included are the section's subheadings to assist the reader in cross-referencing to the text.

> **To coordinate information on the status of year 2000 projects, we recommend that ITD be designated as the central entity to which status reporting from all state agencies and authorities should be submitted. In addition, ITD should establish accreditation methodologies and standards to certify the completion of year 2000 projects.**

Awareness

> **To achieve a broader spectrum of awareness throughout the Commonwealth, we recommend that the Governor issue an executive order related to year 2000 compliance responsibilities and reporting requirements. The executive order should include additional requirements for centralized reporting for all state entities, and incorporate instructions similar to those outlined in Secretary for Administration and Finance Charles Baker's September 29, 1997 letter (see Appendix 4, page 74). The letter was sent to all executive branch secretaries and department heads regarding year 2000.**
>
> **To ensure that all entities become sufficiently aware of the year 2000 problem and how to address it, the Commonwealth should continue its efforts to provide year 2000 awareness seminars across the state. All reasonable efforts should be made to contact those entities that have not been confirmed as having assessed the impact of year 2000. Efforts should be focused on identifying and targeting entities that have not responded to the Fiscal Affairs Division's request for year 2000-related cost estimates, have not been interviewed by ITD's Y2K PMO, or have not attended year 2000-related meetings sponsored by ITD or the Department of Revenue.**
>
> **To keep informed of what other parties are doing with regard to the year 2000 problem, entities should network with each other, consult with ITD's Project Management Office, attend Y2K user group meetings, and use Internet websites as an additional source (see Appendix 5, page 75), such as: Http://www.magnet.state.ma.us/y2k/ and Http://www.isaca.org/yr2000.htm**

Assessment

> **To ensure sufficiently comprehensive impact assessments, entities should assess the entire operational IT environment, including traditional and nontraditional business systems,**

equipment with embedded software across all platforms, and external systems supporting the entity's business functions.

To ensure that year 2000 projects can be adequately planned; systems properly triaged; and realistic cost, resource, and time estimates developed; state entities must devote sufficient resources to complete their detailed year 2000 impact assessments as soon as possible. Entities not having adequate resources to complete their assessments and develop corrective strategies should contact ITD's Year 2000 Program Management Office for advice and assistance.

To help ensure that appropriate controls can be designed and implemented over the IT environment, we recommend that a risk analysis of threats and exposures be performed on current systems and IT operations considering projected risks and exposures during the year 2000 project.

As part of the assessment phase, we recommend that state entities prepare a complete inventory of printed stock where the date fields are preprinted with "19." A plan should be devised to allow this stock to run down by the turn of the century. Where heavy use is anticipated, a run of interim forms with no preprinted century should be considered for use before preprinted forms with "20."

Based on the results of the assessment phase, we recommend that entities prepare and make available a statement of year 2000 impact on the citizens, other entities, and other recipients of state services provided by the entity's information technology. The statement of impact should also be used to guide the development of contingency plans.

To help ensure that important instructions are not lost during software fixes to date fields, entities should determine during assessment the extent to which the values "99" and "00" have been used in date fields to signify something other than dates.

To effectively manage subsequent date-related modifications in a timely manner, a complete inventory of workarounds with sufficient information should be maintained and cross-referenced to the entity's IT strategic plan.

Planning

To help ensure that required resources will be obtained in a timely manner, that costs will not be increased due to lost opportunities, and that required contingency plans will be developed for systems that may not be ready in time, state entities should complete their detailed year 2000 project plans for their entire IT environments as soon as possible.

To assist in developing year 2000 project plans, entities should benchmark against those remediation practices that have led to successful year 2000 projects, incorporating them when appropriate within their own projects.

To help ensure that year 2000 efforts are properly directed, entities should prioritize systems based on their level of mission-criticality, level of risk of malfunction, potential exposure from non-compliance, and complexity of achieving year 2000 compliance. Management should consider focusing compliance efforts on mission-critical systems; evaluating the consequences of noncompliance for less critical systems; and developing appropriate contingency plans to address needed services.

Entities supporting complex and/or multiple software systems should assess the need for using software configuration management techniques. If software is to be used to perform or manage this function, it should be implemented at the beginning of the year 2000 project (or earlier), and staff should be trained in its use upon its implementation or as soon as possible.

With respect to date processing objectives, entities should ensure that the systems can process correctly with regard to the leap year, the date variation of which occurs two months after January 1, 2000.

ITD should integrate year-2000 requirements within standards and guidelines issued by the Commonwealth's Committee on Information Technology Standards and Guidelines.

Entities should adopt contract and warranty language developed by the Operational Services Division (OSD) of the Executive Office for Administration and Finance. We recommend that year 2000 contractors be bonded.

To ensure that entity systems can operate in concert with third-party provider systems, sufficient assurances should be obtained that stated plans are being adhered to for year 2000 compliance, that date field formatting is synchronized with entity systems, or that conversion programs are developed in time. Entities should obtain sufficient evidence of year 2000 compliance and business continuity planning validation for third-party information system vendors and business partners to meet the critical needs of the entity.

We recommend that entities consider leasing equipment to provide increased flexibility in upgrading and shifting IT resources, if required equipment has not yet achieved year 2000 compliance.

Entities should identify all printed stock of forms that are pre-printed with "19" in the year fields and plan for a "safe" shift to the year 2000 format by allowing current stock to run down and reorder modified stock in time to change to the 2000 format.

Entities should send a representative to ITD's Year 2000 User Group meetings.

> **Massachusetts Government Year 2000 User Group**
> The Y2K PMO has launched a Massachusetts Government Y2K User Group. Monthly meetings are held on the first Tuesday of the month in the 21st floor conference room, One Ashburton Place, Boston; the schedule of meeting dates appears below.
>
> February 10, 1998
> •March 3, 1998
> •April 7, 1998
>
> For more information about the User Groups, call Marcia King (617) 973-0711.

Until such time as year 2000 compliance is fully attained, information technology acquisition and development initiatives must address year 2000 compliance.

To expedite corrective efforts, year 2000 project plans should identify as soon as possible the priority of required changes and resources, such as additional staff, analytical software, hardware, and third-party assistance.

Given that important systems need to achieve year 2000 compliance, we recommend that management consider setting aside less essential IT-related projects where resources could be reallocated to year 2000 projects. In that light, we recommend that ITD identify ongoing IT projects that are non-mission critical or not mandated by law where associated resources could be reallocated to year 2000 projects. If required, the Governor should consider postponing IT projects not mandated by law in order to free resources for year 2000.

To ensure that the integrity and security of systems and data are maintained, appropriate internal controls must be in effect throughout all phases of year 2000 projects. Especially important, are controls to protect systems and data from unauthorized access and change and to ensure that modifications are reviewed, tested, and approved before being migrated from the test environment into production. Given that persons from outside the entity may be required to have access to systems and data files during assessment and reprogramming, existing security methods may need to be strengthened to address security and operational control objectives. We recommend that state entities require that procurement of all software, hardware, and equipment containing embedded software complies with the requirements of year 2000.

Incorporated within the fabric of each entity's internal control structure should be control objectives and controls to ensure system and data integrity is maintained with respect to year 2000 compliance. Appropriate procedures should be implemented to ensure that program

change controls and program version controls are in place at all times throughout the year 2000 project. We further recommend that entities establish control procedures to ensure that future development and software maintenance attains year 2000 compliance.

We recommend that each entity establish appropriate monitoring controls to track, evaluate, and report on the progress of year 2000 initiatives including the quality of year 2000-related software changes and the viability of modified systems and technology.

We recommend that entities address year 2000 compliance in cooperation with other entities by networking and taking advantage of resources inside and outside of state government.

To ensure that parties who depend on the entity's systems are aware of year 2000 status, the entity should establish a cost/effective manner to keep all relevant parties informed of year 2000 initiatives.

We recommend that the State Treasurer take all prudent steps required to protect the state's private sector equity investments, given the expected disruptions in the publicly-traded equity markets that may be caused by the year 2000 problem.

Responsibilities and Accountability

We recommend that year 2000 be addressed with an enterprise-wide perspective and that the responsibility for year 2000 compliance be assigned to a senior executive or a level of management sufficiently high within the entity to ensure that the project can be accomplished in a timely manner.

To ensure that adequate attention and resources are applied to the year 2000 problem, entities should establish a year 2000 project team comprised of members who are adequately trained, possess sufficient technical knowledge, and have strong communications skills. To ensure that senior management is kept fully aware of key year 2000 issues and problem resolution, the year 2000 project leader should have direct access to senior management.

To oversee and guide the entity's entire year 2000 project effort, year 2000 steering committees should be established at the entity and secretariat levels. At the entity level, the steering committee should be chaired by a member of senior management, have representation from key user departments, and should include the year 2000 project leader. The year 2000 project-team leader should report to the steering committee for review, approval, and oversight of project activities. At the secretariat level, the steering committee should also be chaired by a member of senior management and have adequate representation of entities within the secretariat.

Cost

Entities should work closely with ITD's Y2K Program Management Office and with the Fiscal Affairs Division to establish year 2000 funding requirements before it is too late. As of December 1997, only 61 agencies had reported their funding needs to the Fiscal Affairs Division.

Year 2000 project teams within entities should work closely with their entity's fiscal management to keep them informed of changes in cost estimates as individual projects progress.

Contingency Plans

To help ensure viable operations and protect services, entities should establish contingency plans for all systems for which there is either a likelihood that the systems will not attain year 2000 compliance, or for systems not to be made year 2000 compliant in time.

We recommend that entities strengthen backup procedures for on-site and off-site storage of backup media; determine whether a more aggressive backup schedule is warranted; and exercise dual control over off-site backup copies for all mission-critical and important systems.

System Modification

Legislative initiatives resulting in mandated changes to automated systems should take into consideration the impact on critical year 2000 projects along with the assessment of other usual factors such as cost/benefit, technical feasibility, security, and business continuity planning. Management initiatives, as well, should also assess the impact on year 2000 projects.

Remedial action should be triaged so that the most critical business critical systems attain year 2000 compliance first. To the extent possible, remedial action of various mission-critical systems should be carried out in tandem, and test scripts and test databases should be built as the remedial action process is carried out.

To guide and monitor their year 2000 projects, we strongly recommend that entities use project management techniques.

To ensure that an entity's year 2000 project is given adequate direction, careful consideration must be given to the skills required to manage the project when selecting and appointing the project-team leader. Staff currently in charge of operations should not be expected to lead the year 2000 project, while also carrying out day-to-day duties.

When windowing is to be used, entities need to ensure that year 2000 assignment assumptions used are in sync with other systems, be they internal or external to the entity.

Program Change Control

To ensure consistency in making year 2000 required program-code changes, to provide a means of control, and to provide an audit trail of what was changed, when, and by whom, we recommend that program-change-control software be used on all year 2000 projects that are deemed to be of sufficient complexity.

To ensure that entities can recover from possible errors that may render that code unusable, we recommend that entities maintain full backup copies of files and systems prior to remedial activities.

We recommend that state entities establish control procedures to ensure that future development and software maintenance is year 2000 compliant.

Data Management

To allow access and processing of existing and archival data, we recommend that entities plan for either conversion of such data, or the provision of an alternate means of processing such data.

System Access Security

We recommend that management review access security policies and procedures to determine whether current controls are appropriate.

To ensure accountability, we recommend that managers ensure that individual accountability is enforced and that unauthorized access to year 2000 programs and data is specifically prohibited.

To maintain the integrity and the required level of security over production libraries, entities should have adequate controls in place to protect on-line and archival data files from unauthorized access and modification.

When making year 2000 modifications, especially when third-party vendors are to be engaged, controls must be established and exercised to protect confidential and sensitive data from unauthorized access.

Testing

To ensure the adequacy of testing, we recommend that entities develop and document test and validation plans for each converted or replaced application of system component, and should implement automated test tools and scripts as appropriate to the automated system being made year 2000 compliant.

Entities with large, complex systems should establish a specialized testing and compliance team, with required skill sets, and implement a year 2000-test facility.

Entities should develop and document a strategy for testing contractor-converted or replaced applications or system components.

To ensure uniformity of compliance results, entities should perform unit, system, and integration tests on each converted or replaced system and system component.

Testing should include regression, performance, stress, and forward and backward test procedures, as appropriate.

Entities should track the testing and validation process and collect and use project-related statistics to manage it.

We recommend that entities incorporate user acceptance testing.

We recommend that, in all cases, entities successfully complete acceptance testing prior to the introduction of new software to the production environment and that entities reintegrate the converted and replaced systems and related data with the new software in as timely a manner as is possible.

Implementation of Remediated Software

To expedite the implementation of remediated software, we recommend that entities define their transition environment and procedures, develop and document a schedule for the implementation of all converted or replaced applications and system components, and resolve all data exchange issues and interagency concerns.

To avoid problems when systems made compliant are reintegrated, we recommend that date field formatting be synchronized, or conversion programs established, for data interchanges with third-party information systems vendors and business partners.

Entities should assess the degree to which software tools can be used to prevent and detect importing incompatible date-formatted data.

To ensure proper implementation of remediated software and systems, we recommend that the year 2000 testing and compliance team be assigned the responsibility of validating and certifying test results, providing assurance that the remediated software operates as intended when reintroduced to the production environment, and ensuring that such software functions properly with all internal and external interfaces.

We recommend that entities expedite database and archive conversions, as appropriate.

When modified software is reintroduced to the production environment, we further recommend that entities develop associated contingency plans and update or develop disaster recovery and business continuity plans.

Reporting

We recommend that a system of centralized reporting of year 2000 project deliverables (e.g., correctly modified system code) be developed and implemented state-wide. Compliance status and validation of corrective action should be established and reported to track progress of individual entities and the Commonwealth at large.

Entities should keep their client base informed as to what actions have been taken to ensure year 2000 compliance for systems (and subsequent status), especially when those clients are dependent upon the entity's systems.

Legal Issues

Entities should maintain complete documentation of efforts to assess year 2000 impact including the development of strategies and tactical plans for addressing the issue, and taking remedial action, verifying test results, implementing modifications and technology, informing parties as to year 2000 actions, and assessing the status of information systems and technology. We also recommend that entities maintain careful records of all activities involved in their year 2000 project. This would include, but not be limited to, the year 2000 planning documents, year 2000 steering committee meeting minutes, documentation of decisions regarding mission criticality and importance of affected systems and associated triage decisions, resource and cost estimates and methods of projecting them, project status reports with timelines and milestones, year 2000 project staff organization, staff qualifications, and training provided regarding year 2000 remediation.

The Governor and the Legislature should consult with the Attorney General in considering possible legislation to limit the Commonwealth's liability arising from year 2000-related occurrences.

We recommend that agencies contract only with those vendors that have signed the year 2000 blanket contract language as developed by the Operational Services Division (OSD). Agencies should be aware that OSD has written standard year 2000 contract clauses for contractual agreements, and entities should use these clauses in all new requests for response (RFRs) and contracts.

We recommend that entities perform a potential liability self-assessment with regard to year 2000 noncompliance and begin now to protect against the occurrence of these liabilities

Where software source code is being held in escrow, entities need to ensure that the escrowed copy of the source code is updated to the version that has attained year 2000 compliance.

Appendix 4

Secretary Charles Baker Letter

Commonwealth of Massachusetts
Executive Office for
Administration & Finance
State House - Room 373
Boston, MA 02133

ARGEO PAUL CELUCCI
GOVERNOR
Charles Baker
SECRETARY

TEL: (617) 727-2040
FAX: (617) 727-2779

To: All Secretaries and Department Heads

From: Charles D. Baker, Secretary, EOAF

Subject: Year 2000 Compliance

Date: September 29, 1997

We face a unique challenge in the history of Commonwealth operations – a turn of the century, coupled with heavy reliance on automated operational systems.

Therefore, effective immediately, it is ordered that:

1. Uninterrupted turn-of-century service delivery is each agency's top operational planning priority.

2. The management of each agency of the Commonwealth is responsible for assessing its Year 2000 preparedness and bringing its systems into compliance, or devising replacement and contingency plans for insuring smooth operations through the turn of the century, and having such assessments and plans committed to writing.

3. All purchases by Commonwealth agencies of new software, systems, enhancements or equipment shall be Year 2000 compliant.

4. New acquisitions which do not address specifically identified Year 2000 deficiencies in older systems should not be put forth as "Year 2000" initiatives.

Agencies are directed to review planned and ongoing technology initiatives in light of this directive and suspend all such initiatives which detract from Year 2000 preparedness efforts, other than those specifically mandated by statewide directives or required by law.

The Information Technology Division, through its Year 2000 Project Management Office, will continue to offer assistance to agencies in their Year 2000 compliance efforts. The Operational Services Division is available to assist with technology procurement matters related to Year 2000 compliance. Please feel free to contact these agencies.

Appendix 5
Year 2000 Web Sites

Massachusetts

Massachusetts Executive Office for Administration & Finance	http://www.EOAF.state.ma.us
ITD Year 2000 site	http://www.magnet.state.ma.us/y2k/
Comptroller's Office	http://www.osc.state.ma.us/
DOR's Division of Local Services	http://www.magnet.state.ma.us/dls/
Operational Services Division	http://www.state.ma.us/osd/osd.htm
Office of the State Auditor	http://www.magnet.state.ma.us/sao/edp1.htm

Other States

Alaska	http://www.stateak.us/local/akpages/ADMIN/info/yr2000htm
California	http://www.Year2000.ca.gov
Florida	http://y2k.state.fl.us/
Indiana	http://www.ai.org/dpoc/
Minnesota	http://www.state.mn.us/ebranch/admin/ipo/2000/2000.html
Nebraska	http://www.das.state.ne.us/das_cdp/rfp/inet.htm
New York	http://www.irm.state.ny.us/yr2000/yr2000.htm
Oregon	http://www.state.or.us/IRMD/y2k/year2k.htm
Pennsylvania	http://www.state.pa.us/Technology_Initiatives/Year2000
Texas	http://www.state.tx.us/standards.html
Virginia	http://www.cim.state.va.us/cdc/index.html
Washington	http://www.wa.gov/dis/2000/y2000.htm

Other Organizations

Official Y2K Website	http://www.Year2000.com
Re: Legal Issues	http://www.Year2000.com/y2karchive.html
Info. Tech. Association of America	http://www.ITAA.org
Gartner Group	http://www.Gartner.com
Computer Tech. Research Corp.	http://www.CTRCORP.com
Federal Government Services Admin.	http://www.Itpolicy.gsa.gov/mks/yr2000/y201toc1.htm
Governing Magazine Y2K articles	http://web.governing.com/governing/92000.html
National Assoc. State Information Resource Executives (NASIRE)	http://www.NASIRE.org/conferences/y2k/index.html
LeBoeuf, Lamb, Greene & MacRae L.L.P.	http://www.llgm.com/
Management Support Technology Corp	http://www.mstnet.com/year2000/

Appendix 6

Year 2000 Project Tracking Form

This form should be completed based on the assessment and inventory phases of a year 2000 project. The form should be updated monthly or quarterly, depending upon the number of mission critical and/or important applications. A detailed inventory item, as well as an indication of the tests and modifications that were performed should support each percent. Management's ultimate goal is to attain 100% in each block.

Y2K Plan □ Drafted □ Approved □ Implemented

Hardware				
	Mainframe	**Minicomputer**	**LANs**	**PC**
Total Number Of Units				
Y2K compliant				
Inventory	%	%	%	%
Program	%	%	%	%
Test	%	%	%	%
Implement	%	%	%	%
Software				
	Mainframe	**Minicomputer**	**LANs**	**PC**
Total Number Of Units				
Y2K compliant				
Inventory	%	%	%	%
Program	%	%	%	%
Test	%	%	%	%
Implement	%	%	%	%

Appendix 7

GLOSSARY

Acceptance Testing
Testing performed on a new or modified computer system as a condition for final implementation or purchase of the system. The tests focus on functionality, data integrity, and internal system controls and the applicability of the needs of system users.

Automated Systems
A series of tasks performed by a computer as opposed to a manual system, which is a series of tasks performed by a human.

Awareness
A phase of a program life cycle. A major drawback of the year 2000 problem is the lack of awareness that agencies, departments, and authorities have regarding applications, business functions and the relationship between a business function and the enabling applications. Understanding the relationship between the business function and its enabling technology is the first step enabling the assessment of the risks, costs, and time requirements in addressing the year 2000 problem.

Backward Compatibility
Backward compatibility refers to an entity's information system's ability to read and process data generated by the system from prior periods. Access may be to four-digit-year-2000-compliant year fields, as well as access to and processing of non-compliant data with two digit year fields.

Benchmarking
A process of analyzing similar organizations, or functions or processes performed by other organizations, in order to attain an understanding of "best practices" to compare to one's own organization, or processes within.

Blanket Contract
A blanket contract is one that is placed at bid and negotiated by the state's Operational Services Division (OSD). By using the state's bargaining and purchasing power in the development of blanket contracts, the best competitive price, terms, and conditions can be obtained and made available to all state entities.

Bridge Program
A bridge program is software written to translate date-related data between compliant and noncompliant application systems or to reformat date-related data for commonality between two or more compliant systems.

Business Partners
Private firms or other government entities with whom an entity shares or obtains products or services necessary for critical operations. Specifically for the year 2000, the data from these partners may be imported into entity computer systems, thus impacting the entity's ability to be year 2000 compliant. It also might include business partner services or products that may not remain available to the entity, should the business partner not be year 2000 compliant.

COBOL
Acronym for a programming method known as "Common Business-Oriented Language" that was developed by the Conference on Data Systems and Languages for use in business data processing applications.

Compiler
Computer software that translates human-readable computer programs (source code) into executable code (a format understandable by the computer to process the program's functions. This translated version cannot be read by computer programmers, thus it is essential that the versions of the computer programs, prior to translation, are backed-up.

Date-Sensitive Fields
Date-related data fields stored in a computer file or in a variable kept temporarily in computer memory. For example, a birth date or years of employee service as calculated based on employee hire and current dates. Date fields are sensitive to the year 2000 issue because their composition may have a two-digit year instead of a four-digit year. For example, we may want to enter a date into a computer system of June 16, 2001. Currently, most computer systems are designed to store the date as 06/16/01. Thus, the computer cannot distinguish whether the date should be June 16, 1901 or June 16, 2001, causing a year 2000 problem.

Decompile
Decompiling a program's object code is the reverse process used when compiling a sequence of source code. Because the process may be prone to error, it should be used only when the original source code is lost and as a last resort. (See also source and object code definitions).

Deliverable
The end result or output of a specific task or group of related tasks. For example, payment checks to vendors are deliverables of the accounts payable process.

Documentation
Reference material that documents how a computer system operates and describes each of its components. It is the primary means by which the knowledge of entity staff is recorded, thereby becoming a permanent entity asset. Documentation may describe computer systems as a whole, how individual programs work, or the purpose and valid values of individual data fields.

Entities
Entities, as used in this report, refers to all state agencies, secretariats, departments, divisions, offices, authorities, educational institutions, boards, commissions, councils, and committees. Entities may organizationally reside within the Executive, Legislative or Judicial Branches, Constitutional Offices, or independent authorities.

Evaluation
A phase of a program life cycle. It is the entity or department administrators' responsibility to evaluate their needs in regard to the Year 2000 project requirements and, if required, to develop appropriate standards, policies, plans, and procedures to ensure the continuation of operations beyond the end of the century. A high-level risks and exposures assessment, and an evaluation of the criticality and importance of each application system should be included.

Examination, Analysis, and Solution Design
Phases of a program life cycle. Information technology, including all critical and important software, hardware, firmware, microcode, operating systems, application systems, job control language, software compilers, queries, procedures, calls to other programs, screens, databases, and data must be examined; analyzed for year 2000 problems; and then a solution must be designed to correct the problem. Software products are available to locate date fields and to simulate what will happen after December 31, 1999. An analysis of system change prioritization and required resources should also be done at this time, including additional staff, analytical software, outside assistance, cost, and time-frame requirements for subsequent phases.

Failure Date
The date upon which a system's functionality is anticipated to be impaired due to its inability to correctly process dates beyond the year 2000. The failure date may actually be before the year 2000 for systems that record future dates - for example, a drivers' license system may currently contain license expiration dates beyond the year 2000.

Field
A data element within a computer file. For example, one's last name is one field within a record containing one's name, address, etc. The inability of specific date-related fields to accommodate a four-digit year might cause the bulk of an entity's Year 2000 problems.

Firmware (operational equipment)
Equipment used in carrying out entity business, which contains imbedded computer processors. Some of this equipment may internally process dates, thus posing a risk to the entity that the equipment may not operate properly near or after the year 2000. The types of equipment include endless possibilities such as: hospital equipment; internal telephone systems; automobiles; and automated equipment such as valves, air conditioning controls, security systems; etc.

Forward and Backward Testing
Forward and backward testing is accomplished by first advancing the computer's internal clock to a date beyond 12/31/99, and then processing with dates solely in the 20th century, performing calculations combining dates from the 20th and 21st centuries, then processing with dates solely form the 20th century other tests as appropriate. The system clock is then reverted to today's date, and the same, or similar, tests are repeated.

GPS (Geographical Positioning System)
GPS is a system of geosynchronous satellites that can indicate the location of an object anywhere on Earth. The system was put in place in the first instance for military use, but has been adopted for many civilian purposes.

Hardware
Items of computer equipment that comprise the physical machines on which computer software operates.

HVAC
HVAC is an acronym for heating, ventilation, and air conditioning.

In-House
Refers to an organizational unit or function performed within the organization, as opposed to third-party provided, or outsourced. An indication that a computer system (primarily computer software) was developed by the entity, with little or no assistance from outside sources.

Infrastructure
The computer hardware and related equipment that comprise an entity's means of processing computer information. This may include computer networks, telecommunications systems, etc. It is important to note that this would include the facilities of a third-party that provides services to an entity.

Information Technology Division (ITD)
A Division within the Executive Office for Administration and Finance. The entity responsible for advising state leaders, assisting agencies, and promoting efficient systems with respect to information resources technology.

Integration Testing
System testing which focuses on the integration of related software modules and applications.

Inventory
The identification of all computer equipment, equipment containing embedded software, and software. It is important for entity or department administrators to have a complete and accurate inventory of their information technology and systems prior to beginning an evaluation of the dimension of their year 2000 problem. The inventory of automated systems would identify the purpose of each system and its relationship (interface) with other entity business elements and systems. The inventory should include descriptive information of each system that can be useful for risk-ranking the system for year 2000 projects. Such information might include: the presence of date-sensitive fields; the size of the system (in terms of the number of computer programs, etc.); the business function supported by the system; and the potential impact of system failure on entity operations and clients served.

Legal Assessments
An identification of possible sources of litigation should entity computer systems or operational equipment fail due to an inability to correctly process dates beyond the year 2000. The assessment should be based on the Inventory of Information Systems, along with an inventory of year 2000 susceptible operational equipment. For example, the assessment might project probable litigation should state-maintained, timed traffic-light systems malfunction due to an inability to process dates beyond 2000.

Microcode
A technique for implementing the instruction set of a processor as a sequence of microinstructions, each of which typically consists of a number of bit fields and the address of the next microinstruction to execute. Each bit field controls some specific part of the processor's operation, such as a gate that allows some functional unit to drive a value onto the bus or the operation to be performed by the Arithmetic and Logic Unit of the central processor. Several microinstructions will usually be required to fetch, decode and execute each machine code instruction ("macroinstruction"). The microcode may also be responsible for polling for hardware interrupts between each macroinstruction.

Milestones
A key point in the progress of a project, such as a delivery date, deadline, or significant point of achievement. This may be the completion of a specific system development phase, such as system assessment, design, computer programming, or testing, for example.

Mission-Critical
Computer based or dependent systems essential to providing key / critical entity services or functions mandated by law. For example, the benefits payment system is essential for the Division of Employment and Training to maintain the ability to distribute unemployment benefits.

Modification
Refers to a change in any component of an information system, typically to program code. It is a phases in the system development life cycle for major changes to automated systems. Programming changes are carried out by in-house and/or vendor programmers and others consistent with the designed solution. During this phase, and subsequently, management must ensure that adequate internal control is maintained over system and data security, confidentiality, and all program changes and versions.

Noncompliance (year 2000)
The state of being unable to process data and calculations because software or firmware cannot differentiate date fields as being between centuries.

Object Code
Object code is the computer machine-readable instructions that are produced after "source code" is run through a program known as a compiler. Object code represents computer instructions in a series of zeros and ones (binary code), which can be viewed as a series of on or off switches combined in patterns to represent letters or symbols.

Operating System
Computer software that controls the operation of a central computer or a personal computer. A computer cannot function without the operating system . On a central computer, the operating system controls requests for access to software and program and data files. Examples are IBM MVS for mainframes, and Novell NetWare for local area networks.

Operational Equipment (see firmware)

Operational Services Division (OSD)
OSD is the state's primary purchasing agent. OSD has written standard contract clauses and warranty language regarding year 2000 compliance as a standard requirement for doing business with the Commonwealth.

Out-sourced
The opposite of in-house. An indication that a computer system (primarily computer software) was developed by a third-party vendor, with little or no assistance from the entity. This could also refer to a computer service provided by a third-party.

Platform
A platform is a computer, most often a mainframe computer, or group of computers on which an entity's applications operate.

Production Environment
The term production environment refers to the storage area within the computer where the set of programs reside that actively operate the data processing functions of the entity. The production environment is usually differentiated from the test environment, where system modifications are tested before being used in production or actual operations.

Regression Testing
Regression testing is performed to detect errors that may be inadvertently introduced when modifications are made to a system's software.

Request for Response (RFR)
A request for response is a document within a bidding process whereby an entity advertises, or otherwise makes it known, that it is interested in procuring goods and services as described in the RFR document. This is the first step in procurement using mandated public-bidding procedures, but is frequently used when not specifically mandated as well.

Scanning
An automated process by which diagnostic software is used to review entity computer programs for potential date problems with respect to the year 2000.

Software
The instructions, written by computer programmers, which direct how a computer should process information. It may take the form of operating system or application programs.

Source Code
The software written to automate entity business processes. Source code is presented in the program language used by the programmers to develop the system and is thereby readable by humans. Once written, the source code is translated (also called compiled) into a form is processed by the computer. Documenting source code is critical to ensuring that a formal record exists of an entity's business processes.

State Entities (see entities)

Stress Testing
Stress testing involves subjecting a modified program or application system to a volume and speed of input, processing and output of data that meets or exceeds those expected during actual production operation.

System Testing
A phase of the system development or program life cycle. It is a test of all of the integrated components of an information system. Each complete system, including all units and/or subsystems, should be tested for full operational year 2000 compliance as soon as modifications are completed for the entire system.

Target Dates
Dates on which specific tasks must be completed or events must occur, regardless of project schedule changes.

Task Dependencies
The timing relationship between project tasks that determines the necessary sequence of events. For example, one task must be completed before the next may begin.

Tasks
A project activity or event that has a defined start, end, and duration. The task produces a measurable result or end product.

Telecommunications
The communications networks used in conducting entity business. These systems may carry voice and/or computer data - a distinction is typically made between a standard voice system and a system dedicated to computer data transmission. In assessing Year 2000 problems, it is essential to identify how telecommunications systems interact with computer systems. The entity's internal phone system should also be reviewed for potential year 2000 problems.

Triage
A process to address situations in which more tasks remain to be completed than time and resources allow. Triage identifies what key tasks can and cannot be performed within the given parameters.

Unit Test
A phase of a program life cycle. System testing which focuses on functional and compliance testing of a single application or software module. Units of application programs and/or subsystems should be tested for year 2000 compliance when programming modifications for each unit is completed. During unit, system, and integration testing, the test environments should afford access security controls appropriate to the systems and data being tested.

UTC (Universal Time Coordinated)
UTC is a base time scale that can be used as a standard time measure anywhere on Earth. It is based on Greenwich Mean Time (GMT).

Utilities
Refers to system software programs that provide a wide array of system functions and which supplement operating system software.

Variables
Values temporarily stored in computer memory, as opposed to fields that are normally values stored on a disk, etc. Variables are used to perform calculations, etc., the value of which may change during processing. These can cause year 2000 problems since, like date-sensitive fields, they may not be designed to correctly handle four-digit years. They may also be a hidden problem since values may be passed from one variable to another before finally being stored in a field on a disk file - making it difficult to determine the source of inaccurate dates within a computer file. Year 2000 scanning programs may overlook these variables due to the passing of values from one variable to the next, or due to variable names with are not readily identified as date related.

Windowing
Windowing is a method used to avoid expanding date fields in noncompliant program code. Using windowing, certain assumptions are made within a translation program about two-digit year dates. For example,"00" through "20" may be assumed to be years in the 21st century, while "21" through "99" may be assumed to be dates in the 20th century.

Year 2000 Budget Projections
A spending plan defining an entity's year 2000 information technology projects and related monetary budgets. State agencies are required to submit such a plan to the Fiscal Affairs Division.

Year 2000 Compliant
A computer system (program code) or piece of operational equipment (containing a computer chip) which is able to associate a correct century with a year. For example the years 1901 and 2001 will be unique, where as a year stored as 01 could easily be interpreted as occurring in any century.

Year 2000 Standard (as adopted by ITD)
The standard date format adopted by the Office of the State Comptroller and ITD for electronic data interchange purposes. Acceptable date formats under this standard include CCYYMMDD format.